

The Anti-Money Laundering Complex in Canada – A Private-public Approach to Governance. The compliance role of financial institutions

Major Research Paper

Sabina Mihaescu | 6134453

Supervising Professor: Patrick Leblond

University of Ottawa

Graduate School of Public and International Affairs

July 23rd, 2012

Table of Contents

List of Acronyms and Abbreviations	3
Abstract	4
1. Introduction.....	5
Research Scope	6
1.1 Globalization, governance and private-public partnerships	8
2. What is money laundering and terrorism financing?	11
2.1 Why is money laundering a problem?	13
3. Origins of the fight against money laundering.....	14
4. The AML/CTF regime in Canada.....	17
4.1 Policy framework – Canadian Legislation.....	19
4.2 Implementation of the AML regime in Canada	20
4.2.1 Roles of the public actors involved.....	20
4.2.2. Roles of private actors– the compliance function	21
4.2.2.i A Risk-Based Approach	21
5. Compliance	23
5.1 Corporations as crime fighters - AML as a task of commercially-oriented institutions	26
5.1.1 Financial Policing as a side-job mandated by regulation.....	27
5.1.2. Challenges and issues:	29
5.2. Why do reporting entities comply?	32
5.2.1. Threat of prosecution or regulatory sanctioning	32
5.2.2. Commercial interests and competitive advantage	33
5.2.3. Reputational interests – Preventing victimization.....	35
5.3 Should AML compliance be a government or corporate responsibility?.....	38
5.4. Is the current system really effective?.....	40
6. Conclusion	46
Bibliography	49

List of Acronyms and Abbreviations

AML	Anti-Money Laundering
ATF	Anti-Terrorist Financing
BIS	The Bank for International Settlements
CFT or CTF	Counter-Terrorist Financing or Combating of the Financing of Terrorism
EU	European Union
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network (the United State's FIU)
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial Intelligence Unit
G7	The Group of Seven Countries: France, Germany, Italy, Japan, United Kingdom, United States and Canada
IASB	International Accounting Standards Board
IFRS	International Financial Reporting Standards
IMF	The International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
ML	Money Laundering
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OSFI	The Office of the Superintendent of Financial Institutions Canada
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PCMLA	Proceeds of Crime (Money Laundering) Act - 2000
PCMLTFA	The Proceeds of Crime (Money Laundering) and Terrorist Financing Act - 2001
PEP	Politically Exposed Person
RCMP	Royal Canadian Mounted Police
STR	Suspicious Transaction Reporting
TF	Terrorist Financing
UN	United Nations
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

Abstract

In Canada, anti-money laundering has developed into a concerted effort between public sector agencies and the private sector to prevent criminal funds from corrupting the financial system. Based on internationally accepted norms, the Canadian legislation has placed bankers, accountants and a handful of other professions as the first line of defence against the laundering of criminal proceeds by delegating them the responsibility to implement policy. These business actors are mandated to maintain records of their clients and monitor their financial transactions, then report suspicious financial activity to the authorities. This responsibility clashes with the inherent motive of the private sector to attract customers and accumulate profit; however, the threat of prosecution, a need to remain competitive and reputational risk are meant to motivate them to comply with their entrusted new role as crime fighters. This paper analyzes the role of business actors as agents of surveillance in the fight against money laundering/ terrorism financing and discusses the effectiveness of the system as dependent on the compliance of these institutions.

1. Introduction

Governance roles are no longer the sole purview of governments, be it due to the need for increased flexibility or higher technical resources. Today non-governmental actors, international organizations, civic society or even the private sector are involved in public policy processes that in the past would have been delivered exclusively by the public sector. The fight to stop money laundering is such an example, where legislative measures established a complex collaboration between government departments and private sector institutions. The anti-money laundering and countering of terrorism financing (AML/CTF) regime in Canada is based on the ability of ‘regime partners’ (public and private institutions) to uncover and deter illicit proceeds from getting into the legitimate financial system. Within the regime, the Canadian financial intelligence unit (FINTRAC – the Financial Transaction and Reports Analysis Centre of Canada) is responsible for analyzing financial transactions and providing information to law enforcement that may assist in the investigation or prosecution of money laundering and terrorist financing offences. FINTRAC bases its financial intelligence almost entirely on transaction reports that private sector actors - financial institutions, real estate brokers, accountants and other money-handling businesses - are mandated by law to submit. A report must be submitted to FINTRAC whenever large or unusual financial transactions are suspected to be linked to money laundering. But in order to assess whether a transaction is suspicious, businesses under the reporting obligation (i.e. the ‘reporting entities’) must know and closely monitor their customer’s financial whereabouts. Therefore, the anti-money laundering system depends on input provided by the private sector. However, the reporting obligation has made bankers, real estate brokers, accountants and other professionals into (willing or unwilling) law enforcement partners of the AML regime. Anti-money laundering regulation has therefore made private-sector entrepreneurs responsible for implementing public policy goals.

When private sector actors, such as banks and financial institutions, became the first line of defence in the fight against money laundering and terrorist financing their relationship with clients was transformed. The new surveillance role they were assigned effectively turned them into “the big brothers of the twenty first century” (Verhage, 2011). Reporting suspicious transactions, as well as monitoring their clients in the name of compliance with AML regulation is raising several ethical and public policy issues that the following discussion seeks to address.

Research Scope

This paper will focus on the implementation of AML/CTF rules, on the delegation of public authority to private actors, and on how this assigns them a contradictory role to act as an arm of the state. Looking at the role of financial institutions in particular, the paper seeks to identify the issues raised by the public-private approach to domestic AML governance and assess whether the public-sector-*principal*/private-sector-*agent* relationship is sufficiently balanced to fulfill the policy objectives of the regime. This aspect of the AML regime has received little attention in the literature. In addition, the role change and involvement of private actors in policing of citizens – traditionally a state function - raises concerns in the areas of accountability, power structure and ethical considerations; this is, mainly because the interests and *raison d’être* of the private actors involved do not overlap with those of the public institutions.

Although the paper’s focus is on AML Compliance in Canada, it will also draw examples from other countries that have implemented similar policies based on the Financial Action Task Force (FATF) Recommendations. Because anti-money laundering and anti-terrorism finance measures are being tackled via the same private-sector compliance regime, the two will be analyzed together. In addition the underlying logic for the widely applied ‘know your customer’ and ‘customer due diligence’ principles employed in both AML and CTF raise very similar ethical and

policy issues. Therefore, in this paper ‘anti money laundering’ regime and ‘counter terrorist financing’ regime may be used interchangeably. In addition, the focus will be on the role of, particularly, banks and financial institutions as private sector reporting entities, because in the fight to preserve financial system integrity, these institutions sit at the core of the system and are central to the day to day functioning of the economy (Reuter & Truman, 2004).

Although there are many ways to launder money, such as asset transactions, casino gambling, currency smuggling (FINTRAC, 2011) or property ownership and property upgrading, they are beyond the scope of this paper. Similarly, tax evasion, which may also lead to money laundering, will not be specifically addressed here, but rather referred to indirectly, in the context of funds laundered through financial institutions. The analysis presented here will look at money laundering, and efforts to combat it, mainly in the context of business actors within the financial sector.

After providing a backgrounder on AML and CTF regulation and governance in the international and national context, the paper will then focus on the implementation side of the policy cycle. It will examine the role private actors have been assigned, due to their position as ‘gatekeepers’ to the financial system and evaluate the different interests of the private actors to comply with AML regulation. It will further lay out challenges and issues faced by reporting entities and conclude with a discussion of effectiveness of current AML/CTF compliance measures.

The analysis presented here is not meant to be an exhaustive examination of the AML regime, but rather seeks to zero-in on what the author sees as the most problematic side of implementation and compliance. It is also not meant to equate the Canadian system with that of other countries; however, as Verhage (2011) points out, AML compliance officers working across a variety jurisdictions are likely to encounter very similar moral dilemmas and be faced with similar

challenges as they try to fulfil the tasks they have been assigned by governments committed to the international model of anti-money laundering.

Research Questions

The role of business actors (mainly from the financial sector) acting as agents of surveillance and performing policing tasks is one that seldom enters the public discourse. Therefore the relationship between public and private sector in combating money laundering/terrorism financing warrants some discussion. The burden of responsibility for AML was shifted onto businesses and corporations, but this creates weaknesses in the system. The question then arises: should AML be a corporate or government responsibility? This paper argues that although the private sector has capacity, expertise and may be better positioned to monitor financial transactions, there are not sufficient checks (and incentives) on this role, in the way that a public institution with democratic accountability would have. The government's current mechanisms to verify compliance merely looks at whether measures are in place according to regulation, not whether compliance is performed well, which then leads to the question of whether the current system can support its effectiveness claims.

1.1 Globalization, governance and private-public partnerships

As Boughton and Bradford (2007) asserted after the onset of the 2007 financial crisis, in today's globalized financial markets, where a weakness in a particular country can spread to the entire financial system, "oversight and regulation should be acknowledged as a global responsibility" (Boughton & Bradford, 2007, p. 10). Today financial transactions are almost instantaneous and global financial markets operate 24 hours a day. The international environment

matters because globalization has greatly improved the efficiency of capital transfers around the world for both legitimate and criminal economic activities. As Wiener (1997) relevantly notes:

“The speed and relative ease with which funds may be transferred across borders has intensified the degree of contact along its filaments. While the intent of this model of world society was to highlight ‘legitimised’ transnational contacts, it has become evident that this cobweb is conducive to spreading security threats emanating from nearly all parts of the globe” (Wiener, 1997)

In the context of money-laundering, the interconnectedness in the global economy and the growth of world financial flows meant that efforts to combat the financial crime had to be internationalized. An international regulatory regime and cooperation between countries became essential to fight the constantly evolving money-laundering methodologies. In addition, protecting the integrity of the financial system meant that that a few countries’ tough AML standards would not suffice; a jurisdiction with lax regulation could destabilize the system, because the structure could only be as strong as its weakest link (Gilmore, 2004). The logic emerging in the late 1980s was that countries with weak AML legislation would encourage money launderers to reroute their illegal income to centres with lax regulatory regimes (Blum, 1984). Deterring regulatory arbitrage would necessitate the joint effort of all countries to harmonize their AML/CTF policies.

Cooperation in AML meant not only government level partnerships but also the co-opting of private sector actors, financial and non-financial institutions, affected by money laundering. The involvement of private organizations in public policy is not a new phenomenon. Governance, in the sense of the decision-making process involved in producing and implementing regulation, traditionally the authority of the nation-state, now regularly implies various forms of cooperation of government with private actors, at both the international and national levels. National and international organizations coming together with market actors and consumers play an increasingly

important role in the creation and implementation of laws and regulation in spheres and industries as diverse as the economy, environmental protection, development or security (e.g. see McGrew & Held, 2002; Prakash & Hart, 2000; Clapp, 1998; Avant, 2005).

Governance here refers to the process of cooperative leadership bringing together actors from various milieus: governments, multilateral public agencies, and civil society to achieve commonly accepted goals; the 'governors', whether belonging to the public or private sector, are assumed to be working towards common goals and objectives (Boughton & Bradford, 2007). Public-private sector cooperation arrangements take various forms, depending on the public policy issue at stake: e.g. advocacy partnerships, regulation partnerships or implementation partnerships (Steets & Blattner, 2010). The expertise and processes that each actor can bring to the table have their advantages and disadvantages; while 'public' governance has democratic accountability and is based on long established processes, it can be cumbersome and slow. Private actors have the ability to be more innovative and mobilize resources more swiftly but may lack legitimacy and recognition. While contracted experienced professionals may provide more expedient and cost-effective policy implementation, delegating public functions to private entities is believed to dissipate the accountability of governors and open the door for opportunism or abuse of the delegated authority (Boughton & Bradford, 2007). Private sector involvement in governance is often criticised because it can change organizational behaviour and shift the responsibility hierarchy within the governance system, which in turn can erode the trust in governors (Cooley, 2010).

In the case of the anti-money laundering regime, financial and non-financial institutions, identified as gatekeepers to money laundering and terrorist financing efforts, due to the type of services they provide (FATF, 2001), have acquired the legal responsibility to fulfill public policy goals. In its current form, the AML establishment is premised on gathering, storing, and analyzing

financial records of clients by the private sector that are then submitted to a public sector agency. The cooperation between the private and public sectors in AML is neither a partnership between equals, nor an outsourcing relationship, but what Steets and Blattner (2010) would classify as a policy implementation partnership and should lend itself to what the authors call outcome accountability: results-based performance evaluation. In AML, the private sector is mandated by law to contribute resources to the policy outcome, but more importantly, fulfill a delicate security role: monitoring and surveillance of customers and financial transactions.

Private-public governance arrangements are often criticized for being unaccountable alternatives to existing (democratically accountable) institutions (Steets & Blattner, 2010). Yet, the AML partnership also raises accountability concerns, because it creates a principal-agent relationship between the public regulator and the private sector implementation actors that shifts the responsibility for fulfilling a sensitive public duty to the private sector (expected to put its profit motives aside and act in the public interest). In addition, due to the secretive nature of financial crime there is an inherent difficulty in estimating the value of money laundering in the economy, and, consequently, the true effectiveness of AML efforts.

2. What is money laundering and terrorism financing?

Money Laundering

Money laundering (ML) is a method employed by criminal entrepreneurs to disguise the origins of money obtained through illegal activities. It is a way for criminals to evade the authorities' suspicions while enjoying their ill-gotten gains, and maintaining readily available capital for additional illicit activities. Financial gain is assumed to be one of the main motives to become

involved in a wide range of criminal activities. In order to prevent leaving a trail of incriminating evidence, criminal funds are moved around or change form (from cash to other financial instruments, prepaid debit cards etc.) to make it look as if they came from a legitimate source (FINTRAC, 2011). According to the Royal Canadian Mounted Police (RCMP), money laundering in Canada amounts to somewhere between \$5 and \$15 billion annually (RCMP, 2011).

Money laundering has varying definitions, depending on each jurisdiction, yet it is generally viewed as a key operation of the underground economy. There are three elements to the complete laundering of funds: firstly the introduction of currency into the financial system usually happens via a financial institution ("placement"), then the funds are moved from institution to institution to further separate them from the initial source ("layering"), and at the final stage they are reinvested in an ostensibly legitimate business ("integration") (Schott, 2006). The majority of anti money-laundering efforts target the initial 'placement' stage of money laundering, as it is a lot more complicated to trace the illegal funds once they have penetrated the financial system. AML efforts depend on the requirement for financial institutions and other service-providers to identify the source, beneficiaries and target of money entering the financial system. With a follow-the-money approach, law enforcement can identify and apprehend criminals by pursuing the trail of funds generated by their illegal activity.

Terrorism financing

Terrorism financing (TF) generally refers to providing monetary support for illegal activities that are meant to seriously harm, endanger or kill one or more persons. The techniques used to launder money (such as using multiple intermediaries, shell companies and offshore accounts) are believed to be essentially the same as those used to conceal the financing of terrorism. Conceptually,

money laundering and terrorism financing are directionally opposing processes: money laundering involves concealing the source of illegitimate funds and using them as legitimate-looking ones, while terrorism financing presumably involves concealing the target of legitimately acquired funds (Reuter & Truman, 2004). Yet both ML and TF, while distinct, make extensive use of the financial system in similar ways, so that, generally, the instruments that are used to combat the former are employed to fight the latter.

2.1 Why is money laundering a problem?

Money laundering is detrimental because it enables criminal groups to continue and expand their operations, by maintaining criminal activities profitable and because it erodes the integrity of the financial system (Levi, 2002). In addition, large money flows could affect the overall monetary volume in circulation, thus impacting the economy at the macroeconomic level (Bartlett, 2002). Nevertheless, money laundering has been portrayed as a threat mainly because financial gain means power, and international/transnational organized criminals can use laundered funds to subvert financial systems that are the cornerstone of international commerce (United States Department of State, 2000) and corrupt the legitimate economy (Verhage, 2011). As Kochan (2005) aptly outlines: “those who secretly manipulate the sources and movement of money affect the security of nations and the wealth of people. We are all victims(...) when major financial or commercial institutions with a global reach handle criminal money, the wider economy is debased, and social and political structures devalued” (Kochan, 2005, p. xv).

From a societal perspective, money laundering is a crime that interferes with the good workings of the financial system and also threatens to undermine public trust in state authority. Being able to effectively control criminal activity is, therefore, “one of the preconditions for being

defined as a modern, democratically governed state in control of its economy” (Helgesson, 2011, p. 471)

3. Origins of the fight against money laundering

Money laundering became an international policy issue in the early 1980s after the United States declared the ‘War on Drugs’.¹ As a means to fight the drug trade in the United States, authorities decided the best way to go at it was to tackle drug revenue and money laundering, and so AML became an auxiliary to the fight against illegal drugs (Sharman, 2011b). When the drug trade (and implicitly money laundering) was declared a threat to national security (Morales, 1989), it essentially enabled the authorities to use extraordinary measures to fight it. Building the momentum was the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, *Vienna Convention*, (United Nations, 1988) that signalled the need for international action to tackle crime and its proceeds in a coordinated way. The Vienna Convention, the first treaty-based international mechanism to address money laundering, called on signatory countries to criminalize money-laundering associated with drug trafficking and enact measures to allow international assistance and mutual legal assistance. Later the United Nations’ *Palermo Convention* (United Nations, 2000) on Transnational Organized Crime expanded the definition of money laundering to other criminal activities, beside drug trafficking. Acknowledging the need for more leadership in AML, the G7 countries pushed for the creation of the FATF (Financial Action Task Force) in 1989.

¹ President Nixon created the Drug Enforcement Administration (DEA) in July 1973 to combat “an all-out global war on the drug menace” (The Global Initiative for Drug Policy Reform, <http://reformdrugpolicy.com>).

The FATF dubs itself a "policy-making body" seeking to “generate the necessary political will” to encourage national legislative and regulatory reforms in AML/CTF (FATF, 2012). This transgovernmental network, comprised of 34 member states and 2 regional organizations,² has since served as an international governance mechanism, spearheading collaborative efforts between national financial authorities of member countries to respond to the shared problems and challenges of money laundering. The FATF has sprung eight additional *FATF-style regional bodies* (FSRBs)³ that work to promote and put into practice AML policies in their respective geographical regions. The FATF is now recognized as the de-facto rule maker⁴ in AML with the mandate to develop and promote international standards to combat money laundering and terrorism financing.

The tools of the FATF are its forty *Recommendations* against money laundering -a set of counter-measures covering the criminal justice system, law enforcement, the financial system and its regulation- and nine *Special Recommendations* to combat the financing of terrorism, introduced shortly after the 9/11 attacks (FATF, 2012). Together the *40+9 Recommendations*⁵ became the global AML norm package, that member countries adopted and introduced into their legislation. So far, over 180 jurisdictions (FATF, 2010), including the FATF members, have signed up and

² The current FATF members are: Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Co-operation Council, Hong Kong, China, Iceland, India, Ireland, Italy, Japan, Kingdom of the Netherlands*, Luxembourg, Mexico, New Zealand, Norway, Portugal, Republic of Korea, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.

³ The Asia/Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CFATF), Eurasian Group (EAG), Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), The Financial Action Task Force on Money Laundering in South America (GAFISUD), Inter Governmental Action Group against Money Laundering in West Africa (GIABA), Middle East and North Africa Financial Action Task Force (MENAFATF) <http://www.fatf-gafi.org/countries/> [Accessed 13-Jul-2012]

⁴ The FATF is arguably the most influential AML international body but by no means the only one. In addition to regional bodies that have sprung out of the FATF, other institutions have also been involved in the fight against financial crime. Similar initiatives have since been pursued by other institutions and in other international forums, such as IOSCO, the Bank for International Settlements, the IMF, through regional bodies such as the Council of Europe, the European Union and the OAS (Helleiner, 2000)

⁵ Financial crime is constantly evolving, and at the beginning of 2012 the FATF revised its 40 Recommendations to be better equipped to act against “new threats to the financial system” (the financing of the proliferation of weapons of mass destruction) and introduced new measures to better address the laundering of the proceeds of corruption and tax crimes (FATF, 2012)

committed to working together to fight money laundering and terrorist financing, when the dominant analogy came to be that the chain was only as strong as its weakest link (Sharman, 2011b).

While the rationale for creating anti-money laundering initiatives originally stemmed from efforts to control the illegal drug trade, it is now recognized that laundered funds may originate from other *predicate crimes* (such as robbery, fraud, embezzlement, bribery kidnapping or human trafficking). AML policies are seen as a tool to reduce the predicate criminal activities underlying money laundering, and the logic of anti-money laundering is essentially that, if crime is motivated by financial gain, then attacking the profits will change the incentives structure for the illegal activity and deter criminals from committing the offences (Sharman, 2011b). A secondary goal of AML is that of maintaining the integrity of the financial system (Reuter & Truman, 2004).

Money laundering is said to have increased substantially over the past few decades, with the rise of complex financial institutions providing more scope for white-collar crime, but mostly due to the expansion of criminal activities across state borders (Sharman, 2011b). Some estimates place the cost of money laundering and its underlying crimes at 2 to 5 percent of global GDP (FATF, 2012). As a result, countries all over the world have spent copious amounts of money and energy to try to eliminate the problem by implementing the FATF-mandated measures to criminalize money laundering, enable seizures and confiscation of criminal proceeds, and attempt to catch the offenders when they try to penetrate the legitimate financial system. Although results of AML measures remain difficult to quantify and evaluate, these measures have become increasingly intrusive over time. In the United States, for example, the political climate following the tragic events of September 11, 2001 allowed legislators to impose strict and intrusive new information gathering measures in the name of protecting national security. Banks now have to submit reports to the authorities when transactions seem suspicious or out of the ordinary for their customers, measures that had not been

possible politically prior to the attacks and had been vigorously fought by bank industry lobbyists on grounds of privacy concerns (Levi, 2002). Michael Levi (2002) further observed that after the 9/11 attacks it was no longer politically or socially acceptable to maintain that financial privacy can be valued more than fighting serious crimes and terrorism, and what had once been one of the tenets of the financial world, ‘bank secrecy’, became an almost pejorative term .

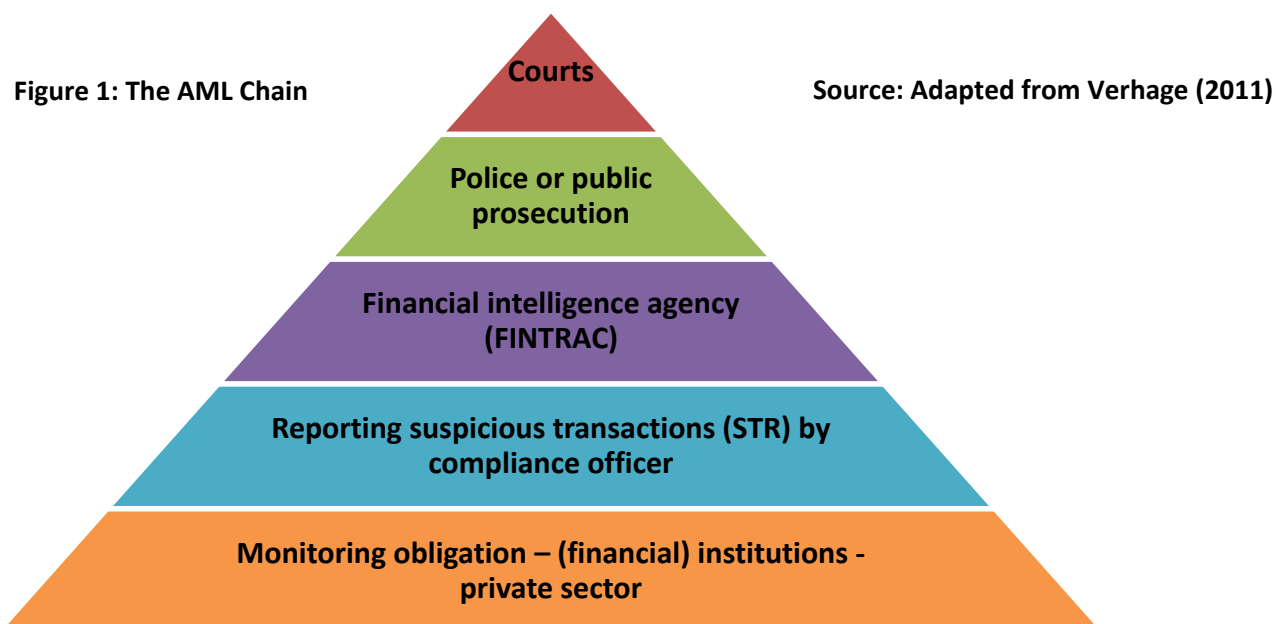
4. The AML/CTF regime in Canada

National initiatives to counter money laundering and terrorist financing introduced in Canada are usually comprised of three distinct dimensions: a regulatory/legal one, an implementation level where the laws and regulations are put into practice through specialized organizations or audit mechanisms and, thirdly, a behavioural level i.e. the development of a corporate culture that mandates the discipline of the banking sector to do its ‘due diligence’ and conduct itself according to regulations (Gysi, 2003). Within the implementation level, countries firstly required risk-prone private entities (financial and non-financial institutions, etc.) to report large or suspicious transactions to authorities, and, secondly, introduced confiscation laws, meant to deter criminals from accumulating financial capital and, implicitly, socioeconomic power (Levi, 2002).

According to Beare and Schneider (2007), the origin of money laundering in Canada dates back to the times of Prohibition in the 1920s and the practice of ‘bootlegging’ – the cross-border illegal trade in alcohol with buyers in the United States. It is believed that a few of these buyers maintained accounts in Canadian banks and had ties with organized crime, making them some of the first money launderers. The development of criminal sanctions and policing powers in Canada has been closely linked to international pressures, especially from its southerly neighbour, who repeatedly singled Canada out as a jurisdiction of “primary concern” and an “international money laundering haven” (Beare & Schneider, 2007). It was also the United States who demanded that

countries replicate the U.S.-style currency transaction reporting system, which feeds information from banks and financial institutions into a financial intelligence unit - a centralized body analyzing suspicious and large financial transactions (Ibid.).

The current Canadian anti-money laundering regime is an initiative made up of the legislative, regulatory and policy framework underpinning the AML/CTF mandates and activities of the *regime partners*⁶ (Canada, Department of Finance, 2010). The entire system, however, rests on the compliance and monitoring obligation of private-sector institutions and businesses. Within these institutions compliance officers, who monitor their client base, submit transaction reports when suspicious or atypical financial behaviour gives rise to concerns of potential money laundering or terrorism financing.



⁶ AML/CTF regime partners in Canada: the Department of Finance Canada (Finance), the Department of Justice Canada (Justice), the Public Prosecution Service of Canada (PPSC), the Financial Transactions and Reports Analysis Centre (FINTRAC), the Canada Border Services Agency (CBSA), the Canada Revenue Agency (CRA) - Enforcement and Disclosures Directorate (Income Tax-GST/HST), the Canada Revenue Agency – Charities Directorate, the Royal Canadian Mounted Police (RCMP), and the Canadian Security Intelligence Service (CSIS). The non-funded partners now include Public Safety Canada (PS), the Office of the Superintendent of Financial Institutions (OSFI), and the Department of Foreign Affairs and International Trade (DFAIT)

Figure 1 illustrates how the anti-money laundering regime works: financial and other institutions monitor clients and transactions and pass their information on to their compliance departments. Here, compliance officers pass their referrals on to FINTRAC, where officials pass on their referrals to prosecutors and law enforcement, which may then refer cases to the courts. The figure also shows how each level is dependent on the one below, and the entire system rests on input provided by the private sector.

4.1 Policy framework – Canadian Legislation

In Canada, the 1989 *Proceeds of Crime Act* first criminalized money laundering and the proceeds of ‘enterprise’ criminal offences and drug offences. The Act also provided civil and criminal immunity to those who *voluntarily* reported to the police transactions where money laundering was suspected (Beare & Schneider, 2007). Then, in 1991, the *Act to Facilitate Combating the Laundering of Proceeds of Crime* mandated that the private sector maintain customers’ records to facilitate the process of criminal investigations; thus financial institutions, banks, credit unions, trust companies and insurance providers had to save client’s information and later, based on a Memorandum of Understanding between the RCMP and the Canadian Bankers’ Association, *voluntarily* report large or suspicious transactions to assist in AML enforcement. The goal was to institute a reporting regime that would aid policing the financial system, and create, as Beare and Schneider (2007) claim, a repository of financial information. These client records kept by the private sector would arguably allow government agencies to uncover evidence about criminal funds and their sources.

Due to international pressure, Canada changed its voluntary reporting requirements into mandatory ones by adopting the *Proceeds of Crime (Money Laundering) Act (PCMLA)* in 2000.

Additionally, after the Terrorist attacks of 9/11 and the nine Special Recommendations issued by the FATF against terrorism financing following the events, Canada amended its legislation to include the new provisions to fight terrorist financing, by passing *the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*.

The operation of the current AML/CTF regime has a wide impact range and is governed by the terms of the *PCMLTFA* but also by other provisions included in the *Criminal Code of Canada, Customs Act, Charities Registration (Security Information) Act, and the Income Tax Act*, among others (Canada, Department of Finance, 2010)

4.2 Implementation of the AML regime in Canada

4.2.1 Roles of the public actors involved

The objective of Canada's *PCMLTFA* is to deter and detect money laundering and the financing of terrorist activities, prevent illicit funds from compromising the Canadian financial system's integrity and provide law enforcement officials the information necessary to prosecute ML and TF offences. The Canadian AML regime requires the cooperation of many government departments and agencies.⁷ However, some play a stronger role in ensuring due process. For example, the Department of Finance Canada has overall responsibility for the AML/CTF Regime; the RCMP is tasked with investigating ML/TF cases, laying charges, making arrests, and seizing funds suspected of being proceeds of crime or that are intended for terrorist criminal activity; the Canada Border Services Agency (CBSA) must ensure that currency or other monetary instruments over \$10,000 that cross the Canadian border are declared and reported to the Financial Transactions Reports Analysis Centre of Canada (FINTRAC) (Canada, Department of Finance, 2010).

⁷ Ibid 6

FINTRAC, Canada's financial intelligence unit, was established as an 'arm's-length' agency, separate from law enforcement and intelligence bodies, in order to retain its independence from political influence. FINTRAC receives financial transaction reports (STR) and produces financial intelligence on suspected ML and TF cases in Canada and abroad.

4.2.2. Roles of private actors – the compliance function

The private actors involved directly in AML in Canada are: banks and financial institutions, money services unions, life insurance companies, real estate brokers, dealers in precious metals and stones, securities dealers, casinos, accountants and British Columbia notaries (PCMLFA). In order to comply with the legislation, these *reporting entities* are mandated to design and implement a 'compliance regime' based on their individual circumstances and business needs. A compliance regime must include: appointing compliance officers, setting up internal AML/CTF policies and procedures, establishing risk assessment methods, perform regular reviews and ensure staff is trained on compliance requirements (FINTRAC Guidelines).

4.2.2.i A Risk-Based Approach

Policy enforcement under the latest Canadian AML act – PCMLTFA- changed the approach to deterring money laundering from one of strict *rules*-implementation to one with an increased focus on *risk* profiles. Before, the public sector established clear, formal reporting rules and criteria for businesses (i.e. any financial transaction that surpassed a certain threshold amount), leaving the regulator to evaluate whether a transaction was suspicious or unusual. All transactions over \$10,000 had to be automatically reported to FINTRAC. However, this requirement could easily be circumvented by transactions below the threshold. Under a *risk-based approach* the private sector

must assess, within their particular business context, which transactions, regardless of amount, pose a risk of money laundering.

The current Canadian AML regime maintains elements from the rule-based approach (i.e. all cash, online or cross-border transactions over \$10K must still be reported) but supplements them with the requirements that reporting entities establish their own policies to assess the risk that their operations will be misused for money laundering or terrorist activity financing. While the risk based approach offers more discretionary power and allows institutions more leeway to develop appropriate internal measures to uncover AML within their client base, it also shifts the responsibility for detection onto the private institution and its compliance officers, and away from public (i.e. government) authorities.

Other countries had already implemented a risk-based approach to their AML system, ostensibly to allow more flexibility to their financial institutions. Yet, at the same time, this has perpetuated a climate of insecurity of financial systems. Anti-money laundering initiatives have focused on criminalization of ML offences and, secondly, on supervising customers suspected of laundering funds, highlighting the securitization⁸ of AML. In Switzerland, for example, the supervisory tactic has evolved from the identification of banking and financial services customers to the verification of beneficial owners of accounts and services. This was in order to go beyond any potential ‘front’ customers and identify the actual recipient and owner of funds (Pieth & Aiolfi, 2003).

However, one of the effects of the risk-based approach, as will be seen shortly, has been that financial institutions are drawn into activities that had previously been the purview of the public

⁸ Securitization here is meant in the sense of elevating a risk to the level of a national security threat (e.g. see Waeber, 2004), and not in the sense of the financial process of issuing of raising finance by issuing bonds or commercial paper.

sector security apparatus: screening citizens according to specific risk factors, anticipating risk, and defining detailed profiles for what constitute threats to domestic and international security. As will be seen in the following sections, this new role for businesses and institutions, expected now to balance public well-being with their primary motive-profit maximization- creates a point of vulnerability in the AML regime.

5. Compliance

Even though the Financial Transactions Reports Analysis Centre of Canada was conceived as an agency to implement the AML regime, it does not have the capabilities to carry out its mandate on its own, and requires reporting entities (private sector actors) to pre-process financial information. This obligation transfers a government responsibility onto corporations and creates a principal-agent relationship between the public and private sector. This begs the question, whether this is a sustainable arrangement, in light of the need for private institutions to balance contradictory incentives: advancing the “public interest” versus augmenting profit for shareholders.

In order to comply with the PCMLTFA, reporting entities subject to the Act must set up internal compliance policies and procedures to properly identify customers, monitor their financial whereabouts, and report suspected financial crimes to FINTRAC. The *reporting entities* – accountants, financial institutions, casinos, securities dealers, real estate brokers, British Columbia notaries, precious gem dealers, life insurance and money services businesses – acquire a legal responsibility to submit suspicious and other proscribed financial transaction reports to FINTRAC. These institutions are required to report not only large cash transactions but also suspicious ones, and they must develop *their* rules for establishing what qualifies as a suspicion, part of the ‘risk-based’ approach discussed earlier. Failure to report suspicious transactions can bring about criminal

penalties of up to \$2 million or 5 years of imprisonment (FINTRAC, 2011). In addition, firms and institutions that send in reports to the FIU are forbidden from letting the customer know that a report has been lodged. In Canada, the criminal penalty for disclosing to a customer that a suspicious transaction has been submitted to FINTRAC is up to 2 years imprisonment.⁹

Effectively the first line of defence in money laundering –bankers, accountants and insurance brokers – have been handed a sensitive legal responsibility that entails getting informed, monitoring and identifying their client’s financial whereabouts and in case of suspected money laundering or terrorist financing, report to FINTRAC. This responsibility to perform a surveillance function on their customers substantially alters the nature of the relationship between client and service-provider in a way that has so far been sparsely analyzed in Canada. The compliance of private sector entities to anti-money laundering regulations has, however, been studied in the AML regimes of France (Favarel-Garrigues, Godefroy, & Lascoumes, 2008), Belgium (Verhage, 2011), Sweden (Helgesson, 2011), the United States (Reuter & Truman, 2004) as well as Switzerland, the United Kingdom and Singapore (Pieth & Aiolfi, 2003) and allows us to draw many parallels to these countries’ regimes.

Anti-money laundering policies represent an effort to make the financial system transparent (Sharman, 2011b), so that the source, beneficiary and target of funds can be kept track of. Naturally, banks and financial institutions were put at the forefront of these efforts and customer identification was seen as a critical component in protecting the safety and soundness of banking systems (Basel Committee on Banking Supervision, 2001). The principle of customer identification (‘Know-your-customer’), first proposed by the Basel Committee on Banking Supervision in 1988, encouraged financial institutions to ascertain the ownership of their accounts and identify clients using safe-custody facilities. This was recommended as a measure to prevent the financial system from being

⁹ FINTRAC: <http://www.fintrac.gc.ca/pen/1-eng.asp>

used as a channel for criminal proceeds (Basel Committee on Banking Supervision, 1988). Customer-due-diligence procedures, formulated by the Basel Committee to further improve customer identification standards, called for proactive account monitoring by banks for suspicious activities and tiered customer oversight (i.e. increased surveillance for higher risk, high net-worth customers) (Basel Committee on Banking Supervision, 2001).

Today, the know-your-customer (KYC) rule extends beyond financial institutions and mandates that all reporting entities establish and record the identity of their clients. Similarly, customer due diligence (CDD) directives are meant to ensure that banks (or any other reporting entity bound in Canada by the PCMLTFA) establish details about their clients such as address, occupation, beneficiary of the funds and relationship with the originator of the transaction. With the introduction of FATF 9 Special Recommendations to prevent the financing of terrorism, the KYC requirement means that clients have to be verified against lists of known terrorists. Virtually the same AML apparatus was to be employed by financial institutions and other money-handling businesses in the private sector bound by these rules, with the addition that they now had to stay alert and be able to evaluate the potential for their clients' terrorist intentions and report on it, or risk legal penalties (Sharman 2011). In Canada the PCMLTFA brought on new provisions that call for the submission of a suspicious transaction report (STR), when there are grounds to suspect that transfers of funds are related to the commission of a terrorist activity (FINTRAC, 2010).

With the implementation of compliance measures banks and other institutions were instructed by the government regulator to perform a vigilance function and monitor customers' financial behaviour. The information thus obtained, would potentially force banks to terminate or refuse business relations with customers. The compliance regulations use banks and other financial institutions as screeners, which places a burden on them to monitor their clients (Chong & López-de-

Silanes, 2007); this is a burden compliance officers feel that governments have unloaded onto them while providing little or no compensation (Favarel-Garrigues, Godefroy, & Lascoumes, 2008). In Belgium 77 per cent of interviewed compliance officers in financial institutions felt that the government saddled the banking sector with governmental tasks (Verhage, 2011). In France, compliance officers thought that delegating this responsibility constituted ‘the ultimate alibi for governmental powerlessness’ as well as ‘a fig-leaf for politicians who don’t really intend to join in the fight’ (Favarel-Garrigues, Godefroy, & Lascoumes, 2008, p. 17). These responses indicate that by delegating this responsibility to private institutions the government may not have suitably resolved the inherent risk and tension that banking officials acting in a dual role of both bankers and detectives, would bring. While some compliance officers admitted that monitoring to this degree could only be performed by banks (Verhage, 2011), others simply felt forced to take on a job they consider extraneous to their profession (Favarel-Garrigues, Godefroy, & Lascoumes, 2008) putting their commitment into question.

5.1 Corporations as crime fighters - AML as a task of commercially-oriented institutions

The AML/CTF compliance function for private-sector enterprises that are under reporting requirements generates a conflict of interest. The FATF Recommendations call for lawyers and law professionals that carry out transactions on behalf of their clients to be included in the list of private-sector actors with reporting obligations. Viewed as potential “gatekeepers” to money laundering and terrorist financing efforts due to the type of services they provide (FATF, 2001) lawyers were seen as frequent elements to complex money laundering schemes. The Canadian legislation first included law professionals in its list of reporting entities, alongside bankers and accountants (Canada, S.C. 2000, c. 17). Canada’s law societies, however, challenged the law, saying it infringed on solicitor-client privilege and confidentiality, and violated fundamental justice principles (CBC News, 2011),

which require that lawyers preserve complete loyalty to their clients. The B.C Supreme Court struck down parts of the PCMLTFA that put clients' interest in jeopardy, if lawyers had to collect information about them and then make it available to the government (Federation of Law Societies of Canada v. Canada (Attorney General), 2011).

The same essential *problematique* applies to the other professionals that are under reporting obligations to the authorities. The AML/CTF regime has delegated to financial and non-financial institutions the duty to protect the financial system, under a threat of criminal prosecution and at a high cost and with little compensation (Beare & Schneider, 2007). But their primary business interest is profit, which entails maintaining and cultivating the trust of their customers, yet the AML compliance obligation requires them to violate this trust.

Private actors are being asked to recognize would-be criminals and cases of potential terrorism financing, when there is no 'effective profile for operational terrorists' that they could use. There are no clear guidelines as to how to identify characteristics of potential perpetrators - but rather just a list of names compiled by national and international law enforcement bodies. In these circumstances it becomes a challenge to generate a strong evidence report, especially since the front line banking officials are not police officers, nor are they trained in wider law enforcement techniques (Beare & Schneider, 2007).

5.1.1 Financial Policing as a side-job mandated by regulation

This also brings up ethical issues, such as whether a private company to which you entrust your money and savings or expect certain services in return for your fees should be entrusted with a surveillance function. In part there is a question of accountability when something goes awry because who these private entities ultimately answer to are their shareholders, board of directors etc.,

but not their customers. As Helgesson (2011) mentions, the setup where agents that are outside the realms of democratic control are involved in monitoring of sensitive data places new demands on client relationships. This may be different in the case when clients surrender information voluntarily (such as to receive better tailored services and special offers from businesses) because there is a perception of mutual benefit for both the customer and the business (Ibid.). There may come a time when these clients, which are to be monitored due to their being potential criminals, will ask “what’s in it for them” (Helgesson, 2011) when giving up information about themselves to banks and financial institutions.

The change in incentive structure is also tricky because it assumes that security motives are stronger than profit motives for these enterprises. But a corporate philosophy of social responsibility to fight money laundering for banks is in a clear tension with profitability, the latter taking precedence over the former. This is because illegally acquired money deposited in a bank, do not inherently harm banking operations; on the contrary, the more and the longer the illicit funds remain in the bank, the more profit they generate for the bank (Beare & Schneider, 2007).

The delegation of surveillance and profiling authority to banks, financial institutions and non-financial entities that deal with monetary transactions in light of the AML regime, has received little attention and scrutiny, while the process has been fast, smooth and almost under the radar (Verhage, 2011).

The mandate of the banking industry is financial intermediation and facilitating economic activity. But more recently, as the criminal phenomena of money laundering and terrorist financing have been raised to national (and even global) security level threat (United States Department of State, 2004), so financial institutions have been assigned surveillance roles. The financial transaction

reports are submitted by banks to the authorities without the consent of the individuals concerned. The extent of the invasion into personal space and the subsequent privacy issues that are raised do not seem to have entered into the public discourse much, although it should raise both national and international concern. Rather, as Ericson and Haggerty (2006) put it, contemporary politics of surveillance encourage individuals to disclose information about themselves willingly, as a type of concession for being able to enjoy various social benefits: “Surveillance becomes the cost of engaging in any number of desirable behaviours or participating in the institutions that make modern life possible” (Ericson & Haggerty, 2006, p. 12) and should, presumably, just be accepted as a fact of life in today’s society!

5.1.2. Challenges and issues:

The current AML regime setup poses several challenges. One of the main difficulties in achieving its objectives revolves around whether it is truly possible for private enterprises to fulfill their compliance goals, in terms of uncovering unlawful fund transfers. For suspicious transactions, for example, the reporting entity is supposed to look at all transactions over the previous year and other accounts held by the same person; then look at the people that the suspicious person has transacted with, in order to generate meaningful intelligence (Sharman, 2011b). Demetis (2010) points out that profiling and typologies of financial criminals (in particular potential terrorists) must be ascertained from what institutions have available, namely the totality of financial transactions. However these are poor tools for this intent, mainly because the amounts of money required to finance a terrorist attack vary greatly. In addition, true profiling requires knowledge that cannot be applied to financial transactions (Demetis, 2010). Even the FATF admitted in 2002 that theirs may not be the best tools for the task at hand:

“Financial institutions will probably be unable to detect terrorist financing as such. Indeed, the only time that financial institutions might clearly identify terrorist financing (...) is when a known terrorist or terrorist organization has opened an account” (FATF, April 2002, p. 3).

Beyond the challenge that the level of data analysis required poses, private sector organizations are provided with only vague guidelines on how to establish who should be reported on, or not. The current risk-based approach, which allows financial (and other) institutions to establish their own AML/CTF policies tailored to their specific industry, also leaves a lot of room for discretion. Decisions whether a suspicious transaction has occurred can sometimes boil down to a subjective, value-laden estimation based on inadequate information (Sharman, 2011b). In addition, front line bank tellers may wrongly identify as ‘suspicious’ those clients who might just behave hesitantly or reticently; other times they may simply be racial-profiling transactions, i.e. the only indices of suspicion are clients’ country of origin, source of funds or its destination (Beare & Schneider, 2007).

The responsibilities imposed on private actors by legislation transforms them into an arm of the state. Compliance officers from various banks interviewed in Belgium felt that AML implementation is a type of outsourcing by the government, where not just the practical execution of AML regulations is left to the banks but also the responsibility for anti-money laundering is shifted on to the financial institution. In a system where the legislator has unloaded the burden of protection onto society, they worry about a future with more intrusive monitoring program where bankers’ AML obligations will expand beyond organized crime control (Verhage, 2011).

The role of banks has shifted when they became central in anti-money laundering and the fight against crime. Financial institutions have become “one of the big brothers of the twenty first century” (Verhage, 2011), now having the authority to monitor and report on their clients whenever transactions appear abnormal. This constitutes a fundamental shift in the role of the banking system and illustrates how the financial system has been securitized. Similar to the way private security enterprises have taken on the role to enforce public order, so financial institutions policing their customers represents a form of delegating an essentially public function to a private authority. This is eroding traditional state monopoly on these areas (Avant, 2005).

Lastly, there are concerns that AML policies may threaten citizens’ personal rights and privacy¹⁰. Private sector institutions must find the right balance between their customer due diligence commitments, their duties to law enforcement agencies and protecting their customers’ privacy. As Beare and Schneider aptly note, the “various links between money laundering and terrorism must be scrutinized, given the ethical implications for the human rights of those who fall within the radar of over-zealous agencies hunting for terrorist financiers” (Beare & Schneider, 2007, p. 297). However, in a climate of securitization, there are continued pressures to give up more information and raise the level of intrusiveness. A March 2012 report by the United States Department of State recommended that “Canada also should continue to ensure its privacy laws do not excessively prohibit provision of information to domestic and foreign law enforcement that might lead to prosecutions and convictions” (United States Department of State, 2012, p. 75).

The tradeoffs to achieve increased security have put financial institutions into a contradictory position, where in order to achieve greater security through the implementation of anti-money

¹⁰ E.g. see Pasley, (2002) for a discussion on privacy rights and money laundering in the United States.

laundering measures, they have been forced into behaviour that goes against profit-driven motives, such as turning down clients or ending existing client relationships (Verhage, 2011).

5.2. Why do reporting entities comply?

Critics say that the growth of the AML regime has raised “relatively little public controversy” and privacy considerations have rarely been an issue, even though AML has put considerable effort and resources in the collection of information about clients (Sharman, 2011b). Banks, for example, initially resisted increased government intrusion in their interaction with clients. However, criminalization of complicity and a series of prominent cases where financial institutions or their employees were prosecuted for failing to report money laundering, served as a strong signal that the AML regime ‘meant business’ (Reuter & Truman, 2004). The reasons why these entities continue to comply with the AML regime revolve around the threat of prosecution, commercial interests, or reputational concerns. However, we will see that these do not necessarily represent sufficient incentives for banks to continue to do a good AML job. The current incentives may hold in theory, but do not necessarily hold in practice; time and time again banks chose their own institutional interests over the common good.

5.2.1. Threat of prosecution or regulatory sanctioning

The most obvious motives for compliance by financial institutions (and other ‘gatekeeper’ businesses) are fines, the threat of criminal prosecution or being excluded from operating in the sector. Before the more stringent AML regulations of recent years, banks and financial institutions’ AML policies were sparsely enforced, and legal prosecution was rarely deployed against non-compliant institutions, except in the most blatant cases (Sharman, 2011b). Today non-compliance

with AML/CTF regulations and failures to report suspicious transactions may mean substantial fines or criminal penalties for offenders.

Tougher AML measures have had a direct effect on the number of suspicious transaction reports submitted. The significant increase in the number of suspicious activity reports cannot be attributed to a comparable increase in criminal activity, but rather to increased compliance (Reuter & Truman, 2004). In the United Kingdom, for example, the number of suspicious transaction reports submitted jumped from 14,500 in 1999 to 94,000 in 2004 when tougher legislation came in effect; but these were in fact ‘defensive’ reports, where financial institutions were trying to take measures to prevent being incriminated in potential future cases, rather than because they believed ML was in progress and needed to be investigated by police (Kochan, 2005).

How strongly the threat of prosecution has motivated institutions to give up their criminal clients remains difficult to establish. Anecdotal evidence and cases with intense media coverage would suggest that financial institutions are willing to risk sanctions when the profit potentials are large enough (see discussion in Sharman, 2011 and the recent HSBC scandal in Hamilton & Voreacos, 2012).

5.2.2. Commercial interests and competitive advantage

The global convergence of AML/CTF regulation standards has also been pushed by the international integration of financial markets. A domestic institution with global reach, such as a bank in today’s competitive world, must hold itself to the international standards of AML. Financial institutions also seek to minimize potential financial losses and would, presumably, try to minimize the risk of paying the large penalties and fines for non-compliance that would affect their bottom-line.

At the international level, a blacklisted or noncompliant jurisdiction may be shunned by legitimate customers and investors, who may bypass it for 'safer' ones. A decision not to implement AML policies would then result in commercial losses. Similarly, at the domestic level, in a highly competitive market for services, a private institution with low AML norm implementation may be at a competitive disadvantage to other similar businesses with more stringent policies. A strong AML compliance regime and an aura of good reputation may become a drawing point for customers, and thus be in a bank's (or any institution's) best commercial interest.

The reverse may also be true, however. Before AML legislation, domestic and offshore banks had presumably been tolerant of criminal funds circulating through their institutions, without a clear harm observable to them or their economies (Levi, 2002). Masciandaro (2005), for example, observes that some countries chose to delay or simply avoid implementing AML regulations despite the blacklisting threat and he speculates that lax financial regulation could in fact have been a strategic policy. Attracting foreign capital, even if it is of illicit origin, might be a profitable move, depending on a country's structural features and on the endowments of its economy. Consequently, the inflow of foreign capital, despite its illicit origin, could provide a boost to the economy (Ibid.). The same logic could then be applied at the domestic level, where a financial institution (or other reporting entity) that tacitly tolerates money laundering may actually profit economically, despite the prosecution threat. As a proverb goes, "the uncaught thief is an honest merchant"; as long as a private enterprise would not be discovered but maintain a façade of AML compliance, it would be regarded as a legitimate business participant.

5.2.3. Reputational interests – Preventing victimization

The last, and possibly most compelling reason to meet reporting obligations, is to prevent reputational damage, because an enterprise's reputation is directly tied to its customer base's confidence and trust. Assuming that these enterprises want to project an image of professionalism and integrity, efforts will then be employed towards good corporate responsibility.

Financial institutions estimate the risk of money laundering and its negative effects to be considerable. A survey of economic crime administered to businesses in 40 countries revealed that the perceived prevalence of money laundering was significantly higher than the actual occurrence of the financial crime among the companies surveyed (PricewaterhouseCoopers, 2007). The fact that the threat of money laundering (and the perceptions of its negative derivatives like reputation damage) was believed to be higher than its actual incidence rate indicates that banks were concerned about preserving their reputation. In light of the recent financial crisis, businesses, especially financial institutions, have come to perceive credibility and reputation as vital ingredients to their survival, and therefore, their risk of victimisation as higher than during times of financial stability (Ernst & Young, 2009). The focus and discourse on the detrimental effects of money laundering on society and economic activity have also raised the expectations of legislators and the general public. Banks and financial institutions are now expected to conform to ethical corporate governance and business operations principles. In this corporate culture money laundering has become one added liability that a bank has to deal with (Verhage, 2011).

Adding to the reputational risk, FINTRAC, in a process mirroring the FATF blacklisting, can publish on its website the names of institutions, or individuals, who have received a non-compliance penalty or been issued a notice of violation (FINTRAC, 2011). In this process, the risk of getting

‘named and shamed’ as a potential ML/TF abetter was hoped to become too great to be ignored by the private sector.

If a scandal breaks out, the logic goes, and a financial institution is found to have among its clients major criminal figures or corrupt heads of states, the resulting unfavourable publicity would not only embarrass the bank but also undermine its share price. Critics, however, point out that even the most serious scandals and reputational disasters of money-laundering involvement have transient effects on client and public confidence (Sharman, 2011b). Beyond transitory humiliation in the press, reputational damage from sanctions and the associated bad publicity leaves little long-lasting damage. Sharman’s research showed that even in cases where banks had been found guilty of gross money laundering offences, their share prices only dropped slightly and rebound within short amounts of time. As Verhage (2011) speculates, this might be because the market’s confidence in a financial enterprise rests more on its capital solvency and operational efficiency, than, presumably, in a philosophy of socially responsible corporate behaviour. Banks are rational actors who will always try to maximize their revenue and minimize risk. When banks accept to hold the vast fortunes of money launderers and kleptocrats¹¹, the profits they can make from these deposits are likely to be substantial. But financial institutions seem to suffer relatively low reputational consequences for involvement in money laundering, even when caught. The sanction that customers and the market impose on a financial institution for laundering money (i.e. the drop in share-price) leaves only temporary marks on their record and attests to the fact that the reputational risk is largely overstated. Customer’s behaviour of ‘forgetting’ fast and bouncing back to doing business with these institutions implies that the reputational risks associated with non-compliance are relatively low.

¹¹ Such as the fortunes of the former Nigerian dictator Sani Abacha, whose regime stole over \$4 billion and deposited them in banks in the United Kingdom, Switzerland, the United States, Germany, Luxembourg and elsewhere (Johnson , 2000) or Philippine’s Ferdinand Marcos believed to have stashed away over \$10 billion in foreign banks (Komisar, 2002).

Sharman (2011b) further reports on a number of high-profile cases where banks in the United States, France and other Western countries failed to enforce basic compliance rules, accepting large sums stemming from the proceeds of corruption, despite being aware of their illegitimate origins. These cases attest to the ineffectiveness of AML regulations to prevent even the most obvious laundering offences (Ibid.). Examples such as these lead one to believe that despite the stated reputational risks, institutions have more to profit from harbouring money launderers than denouncing them. Consequently, the argument that for financial institutions compliance and trust is more imperative than profit doesn't hold.

This evidence does not bode well for the AML regime, whose effectiveness is clearly jeopardized if compliance is not enforced consistently, or implemented only to save face. Verhage (2011) noted that AML efforts performed by banks in Belgium and France served mainly a defensive function, to protect the image of the bank and protect the bank from getting (inadvertently) involved in criminal activities. Fighting money laundering did not rank in the top three priorities of banks, according to interviews conducted with compliance officers in these countries. Similarly, Beare and Schneider (2007) observed that measures to prevent defalcations (frauds against the banks) were more intensive than efforts to prevent money laundering. They speculated that the prevention of defalcations, which make the bank lose money directly, were prioritized over efforts to control money laundering (which does not per se hurt the bank) because the profitability took precedence over security. While the study was performed before more recent changes in AML legislation, the authors nonetheless found that banks tended to aggressively sanction those employees who 'cost' them money by failing to prevent fraud, but were less strict with those employees who were not diligent in reporting suspected money laundering (ibid).

A compliance responsibility enforced only when it serves the interest of the bank, while better than nothing, generates vulnerability in the AML system. If banks continue putting profitability ahead of their legal responsibility to implement AML and CTF regulation then the regime fails to fulfill its goal.

5.3 Should AML compliance be a government or corporate responsibility?

In light of the inconsistent implementation of compliance discussed above, one has to ask whether anti-money laundering should be entrusted to the private sector. But the question of how feasible it is to impose a surveillance function on private corporations (especially those whose primary operational goals are not security), rarely enters the AML discussion.

The normative underpinning of the belief that private as well as public have a shared responsibility for global public goods, is the assumption that power (and actors beyond the state sphere – such as banks - are perceived as powerful) implies responsibility. This rests on another assumption of the presumed common interest of both public and private sector in sustainable development and societal improvement (Bexell & Mörth, 2010). In the case of anti-money laundering, bankers, accountants and a handful of other private sector professionals, seen as ‘intermediaries’ or ‘facilitators’ because they can play a big role for money launderers, can be seen as powerful. This is due to the aura of ‘legitimacy’ and credibility the status of a lawyer, for example, confers to transactions, therefore diminishing the ‘hesitation on the part of financial institutions’ (Beare & Schneider, 2007). Following Bexell and Mörth’s (2010) logic above, this power comes with responsibility and in the name of ‘societal improvement’ these actors should be involved in the fight to stop money laundering. The direct and recurring contact with patrons

provides these businesses the best vantage point to distinguish the malefactors from the legitimate businessmen (particularly in profiling).

Worldwide AML efforts have made make private-sector enterprises responsible for the implementation of public policy goals (Levi, 2002). There is, however, a clear disconnect between the government's AML objectives and the private sector's interests. Whereas the public actor seeks to protect the financial system from money-laundering, commercial enterprises' primary goal is to generate earnings, rather than implement government regulations. To overcome this principal-agent problem and prevent non-compliance, the AML regime introduced the threat of criminal prosecution - 'coercive incentives' (Johnson, 2005). As mentioned earlier, failure to comply with reporting and other requirements carries the risk of substantial penalties for private corporations subject to AML laws. In Canada, FINTRAC also conducts occasional compliance audits, or 'examinations', to ensure reporting obligations by the private sector are respected. An examination reviews whether a particular institution has a compliance regime in place, whether it respects client identification and transaction reporting requirements and how its policies are put in place (FINTRAC, 2010). Additional penalties may be handed out to institutions who fail these examinations. Yet, even with all these warnings and measures in place, the profit motive may still trump responsibility. This point was glaringly illustrated just recently, when in July 2012 the international banking giant HSBC was linked to money laundering and accused of over a decade of recurring compliance failures (Hamilton & Voreacos, 2012). Lax enforcement of compliance regulation allegedly led to the bank tacitly accommodating the financial transactions of drug revenue, terrorist financing and grand corruption. While the investigation by the United States Senate focused on the bank's North American operations, HSBC, as one of the largest global banking and financial services organizations, is likely to put into question the ability of other financial institutions worldwide to self-regulate. In cases of

confirmed money laundering and clear misconduct on the part of bank officials, financial institutions have often put the fault for non-compliance on corrupt officials who failed or neglected to report the vast amounts of criminal money; yet, Beare (2005) argues that in cases when a self-regulated mechanism within the bank has no effective check on negligent or corrupt employees, then the regulatory system has no viable control. Critics are already claiming that “banks are not doing enough to turn away dirty money and the regulators aren’t doing enough to make them” (Ostfeld, 2012), ultimately jeopardizing the entire AML system’s credibility.

The public-private sector relationship in AML compliance puts business actors in an intricate position at the centre of conflicting claims and attributions (Helgesson, 2011) Ultimately, private actors will act in the interest of their clients and shareholders. It would be idealistic to believe that socially responsible corporate responsibility would trump the pursuit of individual utility and financial gain. In addition, these corporations perform a sensitive surveillance function without adequate oversight mechanisms that government agencies under democratic accountability would have. Therefore, AML compliance should, in this author’s opinion, be left to a government actor.

5.4. Is the current system really effective?

The current AML regime is a serious attempt to tackle a complex globalized issue. While there seems to be no real disagreement on the need to do AML, establishing the effectiveness of the current regime remains an elusive goal. This is because measuring effectiveness presents several limitations: firstly financial crime is inherently a concealed activity so it is not easily quantifiable; secondly, one can only indirectly assess the volume or intensity of money laundering by looking at the seizure/confiscation rates of criminal proceeds; thirdly, fluctuation in money laundering charges

and conviction rates can be attributed either to a fluctuation in criminal activity or to changes in law enforcement effort intensity, or both.

Sharman (2011), for example, argues that the extensive AML regulations in place throughout Western countries are ineffective in preventing “even the most obvious and straightforward cases” of laundering corruption wealth. Funds stolen by the ruling elites of developing countries, millions of dollars in proceeds of corruption and tax evasion, have been accepted and stashed in the west by major banks and financial institutions without major reputational repercussions. The FATF-based AML/CTF framework in most countries operates on the assumption that if their recommendations are adopted, a decrease in financial crime will follow. Instead, most government AML bodies have concentrated on assessing the second-order technicalities of complying with the 40+9 Recommendations of the FATF. This ‘goal displacement’ means confounding the effectiveness of AML measures with the level of their implementation where the “means to an end have become ends in themselves” (Sharman, 2011a) and the existence of the reporting system, the policy goal itself. If there is no quality control of compliance measures, then the extensive and intrusive AML polices amount to a type of ‘security theatre’ - a pretext to create a sense of safety, while not doing much to limit money laundering - or whether they serve as a real deterrent. Critics point out that “AML bodies themselves are peculiarly uninterested in finding out whether the system they administer achieves its fundamental goals” (Sharman 2011, p 38). In addition those individuals who work within the system seem to trust its deterrent abilities too much and do not see the practical value in questioning the current policies; meanwhile, outsiders doubt that the AML regime has made a real difference in the underlying crime rates (Sharman, 2011b). In more extreme cases, sceptics simply concede that “most literature on money laundering effects is pure speculation” (Unger, et al., 2006).

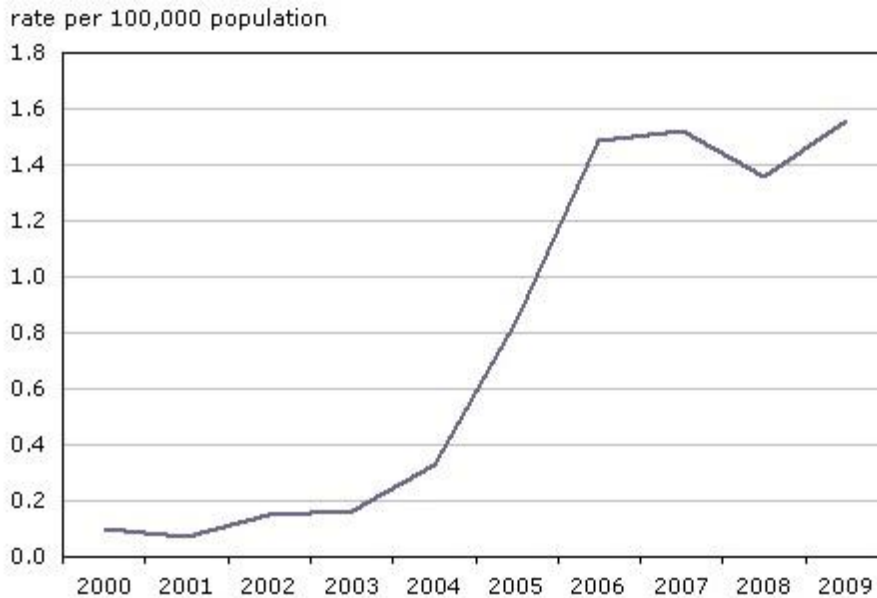
So far there has been no comprehensive attempt to truly evaluate how well the AML compliance measures hold up in the Canadian context. The ten-year evaluation of the Canadian AML/CTF regime undertaken for the Department of Finance in 2010 mentions the effectiveness of the system only parenthetically. The report cautiously mentions that the system “likely contributed to the creation of an environment that is hostile to ML/TF and/or that has been effective in deterring ML/TF and that has reduced the profitability of crime and the likelihood of terrorist activities.” (Canada, Department of Finance, 2010). Senior officials surveyed for the Evaluation opined that Canada’s policies made ML/FT significantly more difficult, as evidenced by reports of criminals’ growing sophistication in attempting to circumvent suspicious transactions reporting requirements (Ibid.). An audit of FINTRAC by the Canadian Office of the Privacy Commissioner only assessed the processes and practices for managing and protecting personal information but did not evaluate the effectiveness of the regime (Office of the Privacy Commissioner of Canada, 2009).

The lack of a comprehensive evaluation of whether the AML system achieves what it was meant to achieve is puzzling. In addition, evidence of evaluations of reporting entities’ compliance measures, generally focuses on the existence of implementation; evidence of quality control of compliance is generally lacking from the literature. In Canada, FINTRAC is tasked with compliance promotion, enforcement and performance analysis of reporting entities and the agency conducts a series of performance audits, ‘examinations’, every year. These are compliance audits meant to determine if the entity is meeting its obligations under the legislation and as the agency’s annual report states, the focus of examinations is “on large entities and high-risk sectors” (FINTRAC, 2011). Unfortunately, the content of these examinations is not published; nevertheless, the 2007 FINTRAC annual report provided some insight in the types of irregularities found among entities audited. At the time, 29 per cent of irregularities uncovered concerned the entity’s overall

compliance regime, 24 percent of deficiencies had to do with failures to ascertain clients' identities and 18 percent were related transaction reporting. The report stated that the vast majority of reporting entities *wanted to comply with the law* and only those persistently non-compliant entities were reported to law enforcement authorities (FINTRAC, 2007). This limited information only allows us to speculate about the level of compliance control that the public regulator exerts. If private sector agents can get away with a 'superficial' compliance to which they may not be honestly committed by claiming, for example, that they *intended* to comply, then they could, realistically, get away with brash AML irregularities. This suggests that private sector entities subject to AML have in fact more leeway to pursue their own interest than the government that set it up had hoped for, which constitutes a real vulnerability of the AML apparatus.

One approach at testing regime effectiveness has been to look at the enforcement pillar and the number of money-laundering offences. Statistics Canada (Brennan & Vaillancourt, 2009) compiled the number of ML incidents over the past 10 years. Money laundering reported by police increased five-fold in the period 2004 to 2006 and then remained relatively stable after 2006 on (see Figure 2).

Figure 2. Money laundering in Canada, 2000 to 2009



Note: Rates are calculated on the basis of 100,000 population. Counts are based on the most serious violation in the incident.

Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey in Brennan & Vaillancourt, (2009)

The dramatic escalation in that two year period has been attributed to a shift in legislative focus along with national and international initiatives aimed at addressing money laundering. (Brennan & Vaillancourt, 2009). This stagnation after 2006 is more difficult to explain; it may well be a sign that ML has not increased in recent years, or that AML measures implemented in recent years have not truly reduced the incidence of the crime. One could even infer that law enforcement has kept the pace of ML advances. This example perfectly illustrates the difficulties in objectively evaluating the current AML/CTF regime's success and effects on the incidence of money laundering.

Jason Sharman tried an innovative way to establish how well AML regimes around the world perform, by undertaking a 'direct test of effectiveness'. He first attempted to form shell companies,

i.e. companies that only have a ‘legal personality’, but no physical assets, employees etc., existing ‘on paper only’. He then attempted, through intermediary law firms and other service providers, to open corporate bank accounts in the companies’ names without providing the required identification documentation – a direct test of ‘Know your customer’ compliance - to see if these service providers would accept. Anonymous shell companies are some of the easiest and cheapest ways to achieve the secrecy needed to hide the illicit financial flows that frustrate AML investigators. Sharman showed that, contrary to conventional wisdom, small-state offshore financial centres were more rigorous at enforcing KYC and customer due diligence rules. Meanwhile big OECD countries and especially the United States (“most self-righteous in the fight against money-laundering” p. 95) were the worst offenders, failing to uphold the international standards that prohibit anonymous companies (Sharman, 2011b). This only shows that time and time again the private sector is one of the weak links in the AML system. By enforcing the rules inconsistently and only when it benefits them, corporations and businesses have shown that the incentives set up by the system are not strong enough to trump their profit-seeking drive. This conclusion is even more troubling in light of the considerable resources invested in the regime; if the regime’s effectiveness is questionable, then the enormous AML industry might eventually impose more costs on society, than the criminals it is supposed to help apprehend (Beare, 2005). In other countries there seems to be the same quandary; a money laundering reporting officer interviewed in the United Kingdom about costs of the AML system there commented that ML sums recovered by the authorities are “negligible and totally out of proportion with the amount being spent on compliance” (Kochan, 2005, p. 255) . The transaction reporting regime alone, purportedly, has come at immense implementation costs for the Canadian financial sector, while it likely detected only a very small fraction of criminal funds, leading Beare and Schneider to assert it has been “the proverbial shotgun approach to killing flies” (Beare &

Schneider, 2007, p. 294). In light of this evidence, any claims of efficiency (as well as effectiveness) of the AML system would not be supported.

6. Conclusion

As the previous discussion has revealed, the anti-money laundering/ anti-terrorism financing system is a very extensive policy, whose efficacy is questionable. There is an inherent tension between the profit motive and security concerns for financial institutions, real estate brokers, insurance companies, casinos and accountants. Banks are organized around attracting funds and there are few rewards for those who turn money away (Beare & Schneider, 2007). Oftentimes the interests of private sectors' in fighting ML/TF may appear to overlap with those of legislators and authorities for reasons identified above (commercial interests, reputational goals); then, private institutions opt to apply measures that protect both the system and themselves against financial crimes. Other times, however, these interests do not fully converge and evidence illustrates time and again that large enough financial gain potential makes businesses shirk their AML responsibilities. The regime is so weak that it would bend its rules in accordance to economic shocks. For example Syal (2009) reports that during the height of the financial crisis in 2008, when lending ground to a halt in the United States and banks were on the brink of collapse, money from organized crime was the only liquid capital available to keep them afloat, demonstrating that when they payoffs are large and the risk is acceptable, financial institutions will close an eye to money laundering. As Verhage fittingly puts it:

"The irony of the implementation of AML measures is, in fact, that banks are as such not harmed by allowing money laundering (passively or by rendering services). Money laundering in itself does not damage commercial interests or pose any financial risks,

Therefore we can hypothesize that without legislation, penal law enforcement and the accompanying reputational hazards, a commercially oriented bank would not be likely to prevent money laundering: criminal money is 'cheap' money for banks as these client probably won't ask too many questions and will not try to grasp all discounts". (Verhage, 2011, p. 38)

The problem is that in the current setup of the AML regime, there is the lack of an effective oversight mechanism to take on the role of quality control for compliance implementation. In addition, there is too much 'stick' and not enough 'carrot' to promote compliance. There are ample penalties and sanctions in the repertoire of regulators, to deter non-compliance; but they are all negative reinforcements that are less effective than positive rewards in promoting rule adherence. Instead, Beare (2005) suggests the government should consider a change in approach that would provide more incentives, observing that only the warning of eliminating bonuses seemed to truly motivate banking officials. She argued for authorities to look into introducing positive reinforcements/rewards for compliance and cautioned that with the current AML regime, one must expect this lack of commitment to continue.

Realistically, there seems to not be sufficient oversight and political will to tackle the shortcomings of the compliance regime. Nevertheless, the government owes it to itself and to taxpayers, after investing substantial resources in the AML regime, to review its policy and attempt to alter the incentive structure for reporting entities. Canada could consider strengthening its AML legislation by getting tougher on criminal offenders and introducing more severe sanctions and penalties. Alternatively it could try to crack down on those reporting entities that are found with deficiencies in their compliance regime and deliver fines rather than warnings from the first offence. If financial institutions can't be trusted to self-

regulate, then a different system of checks and balances needs to be devised to provide a better oversight of compliance processes. Nevertheless, the issue of money laundering is likely to remain a frustrating one for both law enforcement and regulators to address, especially since there is essentially no way to accurately measure the scope of money laundering in the economy and therefore know for certain whether policies are having the desired effect or not.

Bibliography

- Federation of Law Societies of Canada v. Canada (Attorney General), L013117 (British Columbia Supreme Court September 27, 2011).
- Avant, D. (2005, March). Private Security Companies. *New Political Economy*, 10(1).
- Bartlett, B. L. (2002). *The negative effects of money laundering on economic development*. for The Asian Development Bank Regional Technical Assistance Project.
- Basel Committee on Banking Supervision. (1988). *Prevention of criminal use of the banking system for the purpose of money-laundering*.
- Basel Committee on Banking Supervision. (2001). *Customer due diligence for banks*.
- Beare, M. E. (2005). "Voluntary" Ethical Conduct: Anti-Money Laundering Compliance and the Financial Sector. In W. Cragg, *Ethics Codes, Corporations And The Challenge Of Globalization*. Edward Elgar Pub.
- Beare, M. E., & Schneider, S. (2007). *Money Laundering In Canada: Chasing Dirty And Dangerous Dollars*. Toronto: University of Toronto Press.
- Beekary, N. (2011). The International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law. *Northwestern Journal of International Law & Business*, 31(1), 137-193.
- Berdal, M. R., & Serrano, M. (2002). *Transnational Organized Crime and International Security. Business as Usual?* Boulder: Lynne Rienner Publishers.
- Bexell, M., & Mörth, U. (2010). Introduction: Partnerships, Democracy and Governance. In M. Bexell, & U. Mörth, *Democracy and Public-Private Partnerships in Global Governance* (pp. 3-23). Palgrave Macmillan.
- Blum, R. H. (1984). *Offshore Haven Banks, Trusts, and Companies*. Greenwood Publishing Group.
- Boughton, J. M., & Bradford, C. I. (2007, December). Global Governance: New Players, New Rules. *Finance and Development*, 44(4).
- Brennan, S., & Vaillancourt, R. (2009). *Money laundering in Canada, 2009*. Ottawa: Statistics Canada.
- Buethe, T., & Mattli, W. (2011). *The New Global Rulers: The Privatization of Regulation in the World Economy*. Princeton University Press.
- Canada. (2000). The Proceeds of Crime (Money Laundering) Act. Canada.

- Canada. (S.C. 2000, c. 17). Proceeds of Crime (Money Laundering) and Terrorist Financing Act 'PCMLTFA'. s. 1;2001 c. 41, s.48.
- Canada, Department of Finance. (2010). *10-Year Evaluation of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime. Final Evaluation Report*. presented by Capra International Inc.
- CBC News. (2011, September 28). Canada's lawyers exempt from money-laundering laws. *CBC News*.
- Chong, A., & López-de-Silanes, F. (2007). *Money Laundering and its Regulation*. Washington DC: Inter-American Development Bank.
- Clapp, J. (1998). The Privatization of Global Environmental Governance: ISO14000 and the Developing World. *Global Governance*, 4, 295–316.
- Cooley, A. (2010). Outsourcing authority: how project contracts transform global governance networks. In D. D. Avant, M. Finnemore, & S. K. Sell, *Who Governs the Globe?* (pp. 238-265). Cambridge: Cambridge University Press.
- Demetis, D. S. (2010). *Technology and Anti-Money Laundering. A Systems Theory and Risk-Based Approach*. Edward Elgar Publishing.
- Doyle, T. (2002). Cleaning Up Anti-Money laundering Strategies: Current FATF Tactics Needlessly Violate International Law. *Houston Journal of International Law*, 24: 2., 24(2), 279-313.
- Ericson, R. V., & Haggerty, K. D. (2006). *The New Politics of Surveillance And Visibility (Eds)*. Toronto: University of Toronto Press.
- Ernst & Young. (2009). *The 2009 Ernst & Young business risk report. The top 10 risks for global business*.
- FATF. (2001). *Report on Money Laundering Typologies 2000-2001*. FATF.
- FATF. (2008). *Mutual Evaluation of Canada*. Financial Action Task Force.
- FATF. (2010). *An Introduction to the FATF and its work*. Retrieved May 28, 2012, from Financial Action Task Force: <http://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Introduction%20to%20the%20FATF.pdf>
- FATF. (2012, February 16). *FATF steps up the fight against money laundering and terrorist financing*. Retrieved June 20, 2012, from Financial Action Task Force: <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfstepsupthefightagainstmoneylaunderingandterroristfinancing.html>

- FATF. (2012). *Who we are*. Retrieved May 28, 2012, from Financial Action Task Force:
<http://www.fatf-gafi.org>
- FATF. (April 2002). *Guidance for Financial Institutions in Detecting Terrorist Financing*. Paris: Financial Action Task Force.
- FATF Financial Action Task Force on Money Laundering. (2002). *Guidance for Financial Institutions in Detecting Terrorist Financing*. Paris: FATF.
- FATF. (n.d.). *IX Special Recommendations*. Retrieved May 30, 2012, from Financial Action Task Force: <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/ixspecialrecommendations.html>
- FATF. (n.d.). *The FATF 40 Recommendations*. Retrieved May 28, 2012, from Financial Action Task Force: http://www.fatf-gafi.org/document/40/0,3746,en_32250379_32236920_43683560_1_1_1_1,00.html
- Favarel-Garrigues, G., Godefroy, T., & Lascoumes, P. (2008). Sentinels in the Banking Industry. Private Actors and the Fight against Money Laundering in France. *British Journal of Criminology*, 48(1), 1-19.
- FINTRAC. (2007). *Annual Report 2007*. Financial Transaction and Reports Analysis Centre of Canada.
- FINTRAC. (2010). *Annual Report 2010. Ten Years of Connecting the Money to the Crime*. Financial Transactions and Reports Analysis Centre of Canada.
- FINTRAC. (2010). *Guideline 2: Suspicious Transactions*. Retrieved June 20, 2012, from Financial Transactions and Reports Analysis Centre of Canada:
<http://www.fintrac.gc.ca/publications/guide/Guide2/2-eng.asp#s7>
- FINTRAC. (2011). *Annual Report 2011*. Ottawa: Financial Transactions and Reports Analysis Centre of Canada.
- FINTRAC. (2011, May). *Guideline 3A: Submitting Suspicious Transaction Reports to FINTRAC Electronically*. Retrieved June 16, 2012, from FINTRAC:
<http://www.fintrac.gc.ca/publications/guide/guide3a/str-eng.asp>
- FINTRAC. (2011, September 23). *Penalties for Non-compliance*. Retrieved June 26, 2012, from Financial Transactions and Report Analysis Centre of Canada:
<http://www.fintrac.gc.ca/pen/1-eng.asp>
- FINTRAC. (2011, September 20). *What is Money Laundering?* Retrieved May 28, 2012, from Financial Transactions and Reports Analysis Centre of Canada:
<http://www.fintrac.gc.ca/fintrac-canafe/definitions/money-argent-eng.asp>

- Gilmore, W. C. (2004). *Dirty money - The evolution of international measures to counter money laundering and the financing of terrorism*. Council of Europe.
- Global Witness. (2012, July 17). "World's favorite bank" HSBC "left U.S. vulnerable to dirty money". Retrieved from Global Witness:
<http://www.globalwitness.org/library/%E2%80%9Cworld%E2%80%99s-favorite-bank%E2%80%9D-hsbc-%E2%80%9Cleft-us-vulnerable-dirty-money%E2%80%9D>
- Goldsmith, J. (2011, February 21). Explaining money laundering to a Martian. *Law Society Gazette*.
- Gup, B. E. (2007). *Money Laundering, Financing Terrorism and Suspicious Activities*. New York: Nova Science Publishers.
- Gysi, A. (2003). Foreword to Mark Pieth and Gemma Aiolfi.: *Anti-Money Laundering: Leveling the Playing Field*.
- Hamilton, J., & Voreacos, D. (2012, July 17). HSBC executive steps down amid bank links to money laundering around the world. *Financial Post*.
- Haynes, A. (2004). The Wolfsberg Principles - An Analysis. *Journal of Money Laundering Control*, 7(3), 207-217.
- Helgesson, K. S. (2011). Public-Private Partners Against Crime: Governance, Surveillance and the Limits of Corporate Accountability. *Surveillance & Society*, 8(4).
- Helleiner, E. (2000). *The Politics of Global Financial Reregulation: Lessons from the Fight against Money Laundering*. New York: Center for Economic Policy Analysis.
- Hopton, D. (2006). *Money Laundering. A Concise Guide for all Business*. Gower Publishing Ltd.
- Johnson, P. (2005). *Agency problem*. Retrieved June 20, 2012, from A Glossary of Political Economy Terms: http://www.auburn.edu/~johnspm/gloss/agency_problem
- Johnson, T. (2000, November 10). Money laundering exposes Nigeria's oppressors. *World Socialist Web Site*.
- Kahler, M., & Lake, D. A. (2003). *Governance in a Global Economy. Political Authority in Transition (Eds)*. Princeton University Press.
- Kochan, N. (2005). *The Washing Machine, How Money Laundering and Terrorist Financing Soils Us*. Thomson.
- Komisar, L. (2002, August 2). Marcos' Missing Millions. *In These Times*.
- Koppell, J. G. (2010). *World Rule: Accountability, Legitimacy, and the Design of Global Governance*. Chicago: The University of Chicago Press.

- Levi, M. (2002). Money Laundering and its Regulation. *The Annals of the American Academy of Political and Social Science*, 582(1), 181-194.
- Levi, M., & Reuter, P. (2006). Money Laundering. *Crime and Justice*, 34, 289-375.
- Lilley, P. (2006). *Dirty Dealing. The Untold Truth about Global Money Laundering, International Crime and Terrorism* (3rd ed.). Kogan Page.
- Masciandro, D. (1999). Money laundering: the economics of regulation. *European Journal of Law and Economics*, 3, 225-240.
- Masciandro, D. (2004). *Global Financial Crime. Terrorism, Money Laundering and Offshore Centres* (Eds.). Ashgate Publishing.
- Masciandro, D. (2005). False and Reluctant Friends? National Money Laundering Regulation, International Compliance and Non-Cooperative Countries. *European Journal of Law and Economics*, 20(1), 17-30.
- Masciandro, D., Takáts, E., & Unger, B. (2007). *Black Finance. The Economics of Money Laundering* (Eds.). Edward Elgar Publishing .
- McGrew, A., & Held, D. (2002). Introduction. In A. McGrew, & D. Held, *Governing Globalization: Power, Authority and Global Governance* (pp. 1-21). Cambridge: Polity.
- Morales, W. Q. (1989). The war on drugs: A new US national security doctrine? *Third World Quarterly*, 11(3), 147-169.
- Office of the Privacy Commissioner of Canada. (2009). *Audit of the Financial Transactions and Reports Analysis Centre of Canada*. Ottawa.
- Osborne, S. P. (2000). *Public-Private Partnerships: Theory and Practice in International Perspective* (Eds.). Routledge.
- Ostfeld, S. (2012, July 17). Banks falling short on money laundering regulations. *The Hill's Congress Blog*. Washington D.C.: The Hill.
- Pasley, R. S. (2002). *Privacy Rights v Anti-Money Laundering Enforcement*. University of North Carolina School of Law Banking Institute. North Carolina Banking Institute.
- Pieth, M. (2006). *Multistakeholder Initiatives to Combat Money Laundering and Bribery*. Basel: Basel Institute on Governance.
- Pieth, M., & Aiolfi, G. (2003). *Anti-Money Laundering: Leveling the Playing Field*. Basel: Basel Institute on Governance.

- Pieth, M., & Aiolfi, G. (2003). The Private Sector Becomes Active: The Wolfsberg Process. *Journal of Financial Crime*, 10(4), 359-365.
- Prakash, A., & Hart, J. A. (2000). *Globalization and Governance*. New York: Routledge.
- Prakash, A., & Potoski, M. (2010). The International Organization for Standardization as a global governor: a club theory perspective. In D. D. Avant, M. Finnemore, & S. K. Sell, *Who Governs the Globe* (pp. 72-101). Cambridge: Cambridge University Press.
- PricewaterhouseCoopers. (2007). *Economic crime: people, culture and controls. The 4th biennial Global Economic Crime Survey*.
- RCMP. (2011). *Money Laundering*. Royal Canadian Mounted Police.
- Reuter, P., & Truman, E. M. (2004). *Chasing dirty money. The fight against money laundering*. Peterson Institute.
- Ryder, N. (2011). *Financial Crime in the 21st Century. Law and Policy*. Edward Elgar Publishing.
- Savona, E. U. (1997). *Responding to Money Laundering (Eds.)*. Harwood Academic Publishers.
- Schneier, B. (2008). Reconceptualizing Security. *Conference Presentation: Large Installation System Administration Conference*. San Diego, California.
- Schott, P. A. (2006). *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (2nd ed.). The World Bank.
- Schumpeter. (2012, July 18). HSBC's grilling. What comes out in the wash. *The Economist*.
- Sharman, J. (2011a, January 10). A Look at 20 Years of Anti-Money Laundering: Does the System Work? *IFC Review*.
- Sharman, J. (2011b). *The Money Laundry: Regulating Criminal Finance in the Global Economy*. Ithaca: Cornell University Press.
- Steets, J., & Blattner, L. (2010). Partnership Accountability Need Not Be Democratic Accountability. In M. Bexell, & U. Mörth, *Democracy and Public-Private Partnerships in Global Governance* (pp. 55-78). Palgrave Macmillan.
- Syal, R. (2009, December 13). Drug money saved banks in global crisis, claims UN advisor. *The Guardian*.
- The World Bank. (2009). *Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide: Workbook 3a. Regulatory and Institutional Requirements*.

- Unger, B., & van Waarden, F. (2009). How to Dodge Drowning in Data. Rule- and Risk-Based Anti-Money Laundering Policies Compared. *Review of Law and Economics*, 5(2), 953-85.
- Unger, B., Rawlings, G., Siegel, M., Ferwerda, J., de Kruijf, W., Busuioc, M., et al. (2006). *The Amounts and the Effects of Money Laundering. Report for the Dutch Ministry of Finance*. Utrecht School of Economics, Utrecht.
- United Nations. (1988). Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. Vienna.
- United Nations. (2000). United Nation Convention Against Transnational Organized Crime.
- United Nations. (n.d.). *What is Good Governance*. Retrieved June 15, 2012, from UNESCAP: <http://www.unescap.org/pdd/prs/projectactivities/ongoing/gg/governance.asp>
- United States Department of State. (2000). *International Narcotics Control Strategy Report (1999 INCSR)*. Bureau of International Narcotics and Law Enforcement Affairs.
- United States Department of State. (2004). *Money Laundering and Terrorist Financing: A Global Threat. International Narcotics Control Strategy Report*. Bureau Of International Narcotics And Law Enforcement Affairs.
- United States Department of State. (2012). *International Narcotics Control Strategy Report, Volume II Money Laundering and Financial Crime*. Bureau for International Narcotics and Law Enforcement Affairs.
- UNODC. (n.d.). *Tracing dirty money - an expert on the trail*. Retrieved May 30, 2012, from United Nations Office on Drugs and Crime: <http://multimedia.unodc.org/unodc/en/frontpage/2011/August/tracing-dirty-money-an-expert-on-the-trail.html>
- Vandenbergh, M. P. (2007). The New Wal-Mart Effect: The Role of Private Contracting in Global Governance. *UCLA Law Review*, 54, 913.
- Verhage, A. (2011). *The Anti Money Laundering Complex and the Compliance Industry*. Routledge Studies in Crime and Economics.
- Waever, O. (2004). Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery. *Montreal: ISA Conference, March*.
- Wiener, J. (1997). Money Laundering: Transnational Criminals, Globalisation and the Forces of 'Redomestication'. *Journal of Money Laundering Control*, 1(1), 51-63.
- Williams, P., & Vlassis, D. (2001). *Combating Transnational Crime: Concepts, Activities, and Responses*. Routledge.