A Recent Overview of Anti-Money Laundering Organizations within the United States, Canada and Internationally

Tom Cooper
Memorial University of Newfoundland

Ryan Stack
Queen's University

Throughout history, individuals and groups have developed methods to avoid linkages of illicit activities to the money derived from them, largely relying on their ability to conceal their funds, obstruct their source, and integrate them into the legitimate economy. This paper examines recently employed strategies to combat money laundering in the United States and Canada, as well as the roles and responsibilities of two key international organizations tasked with general oversight of international anti-money laundering organizations and the establishment and revision of best-practice recommendations for countries interested in improving their anti-money laundering efforts.

INTRODUCTION

Definitions and Historical Context

Money-laundering, in its broadest sense, is the illegal act of purposefully obscuring the source or owner of an amount of money for the purposes of hiding the commission of a crime, evading taxes, circumventing personal or national sanctions, or avoiding payouts. The practice of money laundering to hide assets from governments may be as old as the concepts of governments and currency themselves; some authors (e.g., Seagrave, 1995) have documented evidence of money laundering amongst ancient Chinese traders, who devised methods of hiding wealth to avoid abuse and confiscation from the ruling class as early as 4,000 BC. It is not hard to imagine that such methods have existed as long as individual wealth and regimes have existed, however codified rules criminalizing money laundering and its related activities are a relatively new development. Presently, the practice of laundering 'dirty' money is most heavily associated with underlying criminal acts, including racketeering, illegal gambling, prostitution and drug dealing. Most definitions refer to money laundering as serving to transfer proceeds of crime into legitimate-seeming assets to allow criminals to access the proceeds of those crimes while avoiding detection by authorities (International Money Laundering Information Bureau, 2015).

Though the prima facie nature of money laundering naturally restricts the ability to determine its total impact, current estimates by the United Nations Office on Drugs and Crime (UNODC) indicate between $800 billion and $2 trillion is laundered worldwide annually, of which less than 1% is discovered and

confiscated (United Nations Office of Drugs and Crime, 2013), in spite of the best efforts of many national and international organizations.

There are many techniques noted by law enforcement agencies as primary methods for conducting money laundering, and doubtlessly many more complex or well-concealed methods yet to be uncovered. In general, money laundering is achieved via three fundamental stages: Placement, Layering, and Integration (See Figure 1).

FIGURE 1
PHASES OF MONEY LAUNDERING

Source: Adapted from World Economy Ecology and Development (2013)

Placement

In this phase, 'dirty' money (i.e., money obtained through criminal activity) is placed into the financial system, thereby relieving the criminal of holding large amounts of cash (Business Crime Solutions Inc., n.d.). This is a crucial step in the process of money laundering, and also the one that is most vulnerable to detection by authorities. Placement may be achieved via a number of common methods, including repayment of loans or credit cards with illegal proceeds, gambling through purchase of chips or bets placed on sporting events, the purchase of foreign funds through foreign currency exchanges, and the physical movement of currency or monetary instruments over international borders (Business Crime Solutions Inc., n.d.).

Layering

This phase, also called structuring, is the most complex of the three, regularly involving international movement of funds. The primary function of this transfer is to obscure the source of the funds, to confuse the audit trail and dissolve any link to the initial crime. Methods utilized at this stage include electronic transfer of funds to a foreign country followed by the division of these funds into complex instruments or other overseas markets, taking advantage of inefficiencies in legislation and lags in cooperation between countries (Reuter, 2004).

Integration

In this final phase, the funds are returned to the criminal, now ostensibly legitimate. The major objective is to reunite the money with its owner without drawing attention to the transfer and while maintaining the appearance of a legitimate source. Extravagant purchases such as luxury automobiles, jewellery or art work, as well as investments in more practical ventures like real estate or existing legitimate businesses often serve this purpose.

Money laundering has assumed a new level of threat in recent years due to increasing concerns of elements linked to terrorism. As a result, many law enforcement agencies have devoted significant time and effort to detect, prevent and punish money laundering in all its forms. These organizations have been empowered through various pieces of legislation to collect, examine and act upon evidence of money laundering. The efforts of these organizations have also been bolstered through increased co-operation facilitated by international initiatives including the Financial Action Task Force on Money Laundering (FATF) and the Egmont group. These initiatives have not been without collateral damage, with anecdotal

stories of prizewinners, newlyweds or legitimate businesspersons running afoul of such organizations continuing to rise. In addition, the increasing zeal with which organizations pursue these activities, sometimes in the absence of evidence of an underlying predicate crime, has led some to decry money laundering as 'financial thought crime' (Matonis, 2013), drawing parallels between the broad scope of the law as applied and the powers held by the authoritarian regime depicted in George Orwell's 1984.

Though the concerted efforts of allied countries throughout the world continue to evolve to address the continuing practice of money laundering, so too do those of its practitioners. The advent of new technologies continually provides novel methods by which criminals may hide the sources of illicit funds. By necessity, the laws surrounding such technologies always lag behind the activities which they enable, as they must be understood, carefully crafted and ratified by a number of interested member states.

Recent History

The Rise of Anti-money Laundering Laws

As discussed above, money laundering, in the form of hiding money from authorities or others who may claim a stake in it, stretches back many thousands of years, perhaps to the very dawn of civilization, which allowed individuals to build personal wealth and created regimes with a declared right to seize a portion of such wealth. Such practices would have traditionally been easy to implement, given the lack of oversight of banking and wealth transfer systems that has historically existed throughout the world.

In some instances, financial crime has served as a proxy to allow authorities to prosecute criminals where it proved impossible to build a case against them for the underlying infraction. Perhaps the most well-known example of this is prosecution of infamous prohibition era gangster Alphonse Capone. Though Capone was never successfully prosecuted for the racketeering, bootlegging or murders of which he was widely suspected, he was successfully convicted for income tax evasion for failure to report this income in his taxes following an investigation by the Internal Revenue Service (IRS). Unbeknownst to Capone or his compatriots, earned income, even that earned through illegal enterprises, must still be declared to the government and taxed at the appropriate rate (Internal Revenue Service, 2015). At the time of Capone's conviction, no laws existed specifically prohibiting money laundering, establishing penalties for the offence if convicted, nor providing law enforcement with the necessary tools to properly investigate suspected instances of the practice.

Capone's conviction sent shockwaves throughout the criminal underworld, leading his former associates to begin laundering money in a systematic and conscientious manner to avoid suffering a similar fate while maintaining their criminal enterprises (Internal Revenue Service, 2015). Illicit activities like drug dealing, arms sales, human trafficking and illegal gambling can yield large sums of money, which must be hidden or 'cleaned' to disguise its true source, and often to avoid paying heavy taxes on it as income. In addition, activities like drug dealing often see goods exchanged in many smaller transactions in exchange for small bills. Currency in such form is difficult to maintain, store and transport, and must be exchanged for larger bills for more efficient storage and distribution, however standard financial institutions may be suspicious of deposits made in this form. Aggregating funds in small denominations into larger bills is therefore a goal also served via money laundering.

Though criminals continued to be pursued by authorities for their underlying crimes as well as the crime of tax evasion, the act of money laundering was not made illegal per se until the passage of several laws beginning in the 1970s. During this time, countries in North America and Europe specifically enacted laws and established organizations to prevent, detect and penalize the practice of money laundering (Internal Revenue Services, 2015). These laws and organizations included both domestic initiatives to combat such practices within individual countries, as well as broader efforts to share information and foster greater co-operation between countries.

Money Laundering Methods – New Technologies

While many increasingly complex forms of money laundering schemes exist, the basic principles remain in place – criminals must mix their illegal funds with legitimate funds, effectively obscure their

source, and then extract that wealth again. A common practice to achieve this goal has been for criminals to invest in legitimate businesses that may naturally expect to receive funds from multiple sources in small denominations. These may include restaurants, bars and laundromats. In fact, a legend within the field states that investments in laundromats by prohibition-era gangsters are what led to the use of the phrase 'money laundering.' Though the validity of this story is questionable, businesses like laundromats do remain a key front for money laundering operations.

The advent of new technologies has offered innovative avenues by which criminals may launder money and shift it from one country to another. Two key methods that are of interest to law enforcement agencies are prepaid access cards, including prepaid credit cards and store cards, which allow convenient transfer of funds to legitimate channels; and the use of electronic currencies like Bitcoin to shift currency from one source to another without detection. These developments remain a major concern for domestic and international law enforcement agencies in their campaign against money laundering.

Prepaid cards were first introduced in 1995 by Blockbuster Video, presented as a convenient method of giving gifts targeted at patrons of the store (Duhaime Law, 2015). Since their inception twenty years ago, such cards have grown exponentially in popularity and scale, with companies of all sizes availing of prepaid programs to promote their brands and lock in cash payments. Conversely, prepaid credit cards first saw release in the late 1990s as alternatives to traditional credit and debit cards which require neither evaluation of creditworthiness nor accounts at a traditional bank (Financial Action Task Force, 2013). The value stored in such cards has likewise grown, with prepaid cards reaching an estimated $200 Billion in 2014 (Groenfeldt, 2014). Money laundering via this channel is a serious risk because no oversight exists on such purchases (Groenfeldt, 2014). Cards can be loaded and re-loaded with values up to the tens of thousands of dollars, with no obligation or mechanism for the individual vendors to report purchases. In addition, the compact nature and ubiquity of prepaid cards means that large amounts of value can be easily and discreetly transferred between parties or across borders. To combat this threat, anti-money laundering organizations throughout the world are investigating their abilities to monitor prepaid deposits as they do other financial services within their individual financial systems. This is a demanding process, requiring the assessment of the risks involved, determination of the burden this would place on businesses involved, and the drafting and implementation of new legislation to encompass the risk area. In this process, authorities must be especially careful not to place onerous requirements that may have unintended consequences for innocent businesses or make sweeping changes that may shock the financial system (Gray, 2014).

A more recent and innovative technological development, virtual currencies, such as Bitcoin, present a unique challenge for Anti-Money Laundering regimes. Virtual currencies have the same basic functions as conventional currency, acting as a medium of exchange and a store of value (Financial Action Task Force, 2014). However, virtual currencies circumvent traditional financial systems, as they are not issued by governments and are not linked to the value of any underlying assets (United States Government Accountability Office, 2014). Virtual currencies offer a high degree of privacy compared to traditional systems, often operating as direct peer-to-peer transfers without a central intermediary to collect and store information. As virtual currency systems have no physical medium and exist solely electronically in the form of computer code, such transfers can be made globally, further inhibiting law enforcement agencies' ability to restrict illicit transactions across borders (Velde, 2013). Virtual currencies present a special challenge for Anti-Money Laundering regimes because of the speed with which they evolve, due in large part to the level of crowdsourcing involved in their development and the commitment of designers to the idea of the medium. This threatens to make such currencies uncommonly difficult to regulate, with the medium able to adapt to circumstances much faster than legislators and law enforcement agencies can develop and implement new rules and regulations.

THE FIGHT AGAINST MONEY LAUNDERING

United States AML Efforts

Bank Secrecy Act

The Currency and Foreign Transactions Reporting Act of 1970, commonly referred to as The Bank Secrecy Act (BSA) was passed in the United States in 1970 (Financial Crimes Enforcement Network, 2013). The BSA represented a pivotal piece of legislation in the fight against money laundering in the United States, as it mandated the co-operation of financial institutions, most importantly federally insured banks and credit unions, to give assistance to government agencies to detect and prevent the practice of money laundering. To facilitate this co-operation, the Act places the onus on such institutions to keep records of purchases of financial instruments or cash transfers in excess of $10,000 in a single day as well as to report activities that are considered suspicious and that may indicate tax evasion, money laundering, or other general criminal activities are being undertaken. These records take the general form of Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) respectively.

By mandating SAR and CTR submission by financial institutions, the BSA seeks to eliminate the availability of such institutions as intermediaries for criminal activities or money laundering, thereby making it more difficult for criminals to hide their illicit profits. CTR documents are fairly straightforward, representing simple recordkeeping of normal activities such as deposit, withdrawal, transfer or foreign exchange of amounts in excess of $10,000. Conversely, SARs are designed to allow a mandated method by which institutions may alert authorities of activities observed in clients which they know, suspect, or have reason to suspect meet any of the following conditions (Financial Crimes Enforcement Network, 2005):

- Involves money from criminal activity
- Is designed to evade BSA requirements, through structuring (designing a transaction to evade reporting or recording requirements) or other means
- Appears to serve no business or other legal purpose and for which available facts provide no reasonable explanation
- Involves the use of the money service business to facilitate criminal activity

The role of a financial institution in filing a SAR is not to accuse customers of acting illegally, it is only to report on activities deemed suspicious for further examination by the proper law enforcement authorities. Institutions are protected from civil litigation resulting from the filing of a SAR, and it is illegal to inform anyone involved in the transaction that a SAR has been filed (Financial Crimes Enforcement Network, 2005). The general process for filing an SAR is laid out in Figure 2: Suspicious Activity Report Filing Process. Suspicious Activity Reports continue to play a vital role in alerting authorities to activities that may indicate money laundering or other criminal activities. As demonstrated in Figure 3: Suspicious Activity Reports 2010-2013, the frequency of SAR filings continues to increase annually. Though an upsurge in reports is apparent, it is unclear whether these increases are a result of increased transactions in general, an escalation in criminal activities or increased vigilance on the part of financial institution personnel.

FIGURE 2
SUSPICIOUS ACTIVITY REPORT FILING PROCESS

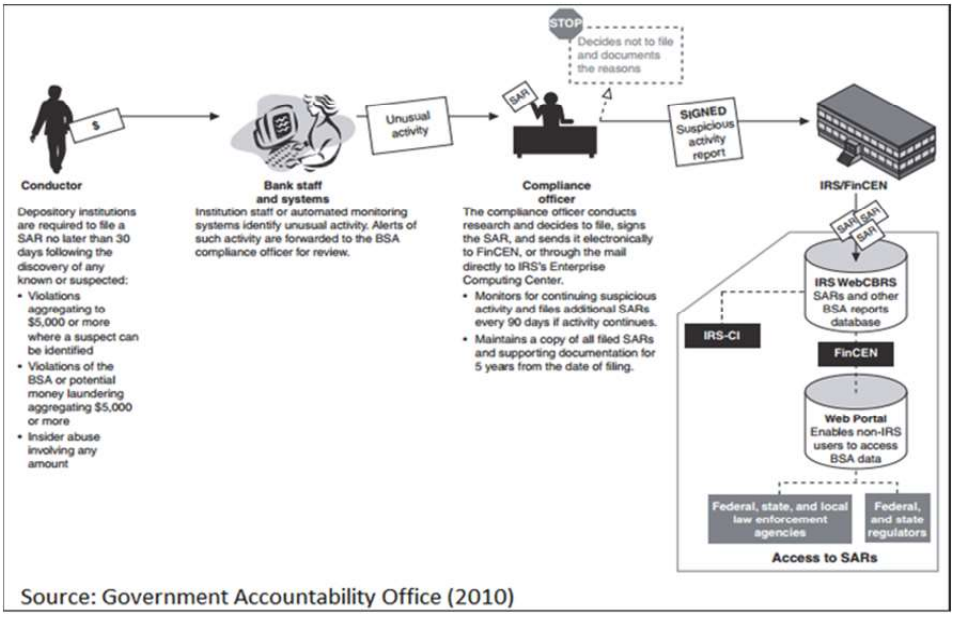
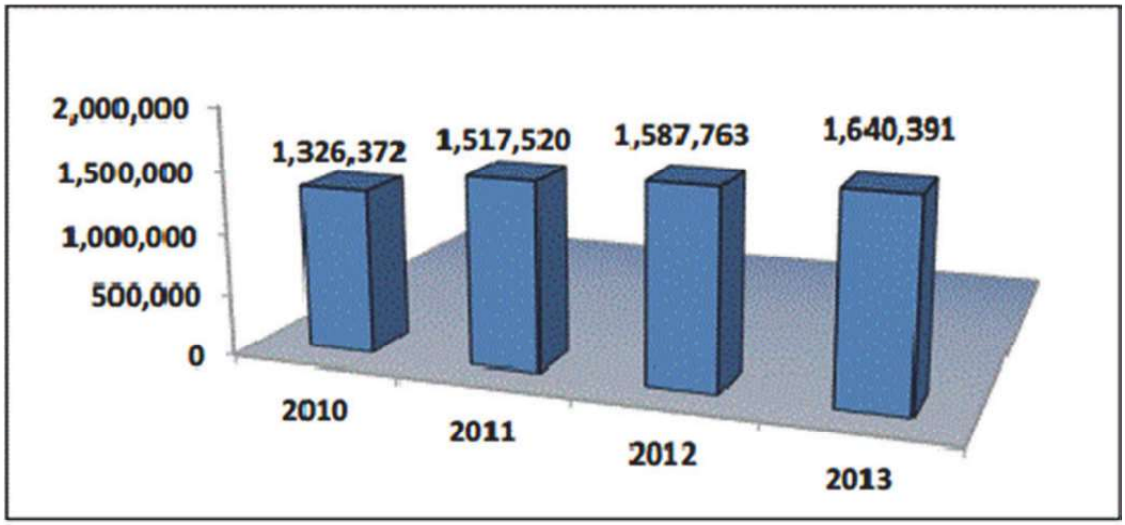


FIGURE 3
SUSPICIOUS ACTIVITY REPORTS 2010-2013



Source: Financial Crimes Enforcement Network (2011)

As shown in the figure, the magnitude of increase year-over-year appears to be declining, with a 2012-2013 increase of approximately 50,000 filings, compared to an increase of approximately 70,000 for the 2011-2012 years. Activities deemed suspicious are not necessarily criminal in nature and may simply represent a desire to avoid being included in a government list or be forced to file paperwork. However, structuring, the act of taking deliberate steps to avoid documentation under the BSA, is an offence in itself. Such activities are exceedingly easy for the government to prosecute, with such cases often resulting in fines, asset forfeiture, or jail time (Internal Revenue Services, 2015). The relative ease with

which prosecutors can indict a citizen for structuring, even as a standalone crime in the absence of proof of ill intent, is something emphasized by detractors of the wide-reaching powers currently granted by the Bank Secrecy Act. In particular, they note the increase of structuring as a standalone charge brought by prosecutors rather than as an ancillary charge linked to underlying crimes has been a concern for defense attorneys and civil activists, who assert that such tactics are abusive and place an emphasis on seizing money regardless of its source (Balko, 2014).

The Bank Secrecy Act has continued to evolve as the needs and attitudes of lawmakers have grown and shifted, and the Act remains a living document. In particular, the Act saw enhancement in the 1980s as the American government sought to aggressively restrict drug trafficking, in the 1990s as law enforcement and intelligence agencies sought greater integration and co-operation from financial institutions and each other, and in the 2000s, particularly following the attacks of September 11, 2001, as the country established links between money laundering and terrorist financing which became a top priority (Financial Crimes Enforcement Network, 2014) Included in these changes has been the evolution of the organization created to enforce and oversee the requirements of the Bank Secrecy act, the Financial Crimes Enforcement Network.

Financial Crimes Enforcement Network

The Financial Crimes Enforcement Network (FinCEN) was originally established in the early 1990s with the mandate to provide a government-wide, multi-source financial intelligence and analysis network. The intention of this network was to act as a central point of contact between financial institutions and law enforcement agencies, allowing them to interact and exchange information (Financial Crimes Enforcement Network, 2014). This enhanced transparency was considered a key component of the battle against money laundering in the United States.

In 1994, the scope of the organization was extended, giving FinCEN direct responsibility for administration of the Bank Secrecy Act, accepting this responsibility after absorbing the Treasury's Office of Financial Enforcement, which had previously been tasked with BSA administration (Financial Crimes Enforcement Network, 2014). FinCEN's powers and scope continued to grow throughout the 1990s and into the early 2000s, before seeing radical changes in the wake of the terrorist attacks of September 11, 2001.

Following the September 11, 2001 terror attacks, the United States Congress passed a broad and far-reaching piece of legislation intended to grant law enforcement and regulatory agencies the necessary powers to prevent and combat terrorism. This law, officially called the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, but better known by its acronym, USA PATRIOT Act or simply Patriot Act (The Act), broadened FinCEN's mandate to include a focus on terrorist financing as well as its long-standing concentration on money laundering (Financial Crimes Enforcement Network, 2012). The Act also placed FinCEN under the authority of the Department of the Treasury (Treasury), with its personnel divided relatively evenly between administrative and managerial professionals, analysts, and personnel devoted to regulatory concerns.

Being under the umbrella of the Treasury places FinCEN as a peer to other financial investigation organizations, including the Internal Revenue Service (IRS), which is responsible for collecting tax revenue for the United States and conducting investigations should there be suspicion of tax evasion, as well as the Office of the Comptroller of Currency (OCC), which is responsible for oversight of national banks to ensure the integrity of the banking system (U.S. Department of the Treasury, 2013). The co-operation of these organizations enhances FinCEN's ability to carry out its stated mandate and assist law enforcement in curbing the prevalence of money laundering within the United States.

In addition to organizational changes, Section 314(a) of the Act made FinCEN a key aggregator of information and go-between allowing communication between federal law enforcement agencies and financial institutions. These communications have greatly enhanced the ability of law enforcement to reach out to more than 43,000 contact points in over 22,000 financial institutions, allowing them to locate accounts and examine transactions of persons suspected in terrorism or money laundering (Financial

Crimes Enforcement Network, 2015). This unprecedented co-operation between law enforcement and financial institutions leverages technology to collect, analyze and act upon disparate pieces of information, revealing patterns and activities that would otherwise be impossible to determine. Law enforcement feedback shows that since the program's start in 2002, approximately 95% of 314(a) requests have resulted in arrests or indictments (Financial Crimes Enforcement Network, 2015).

Canadian AML Efforts

Canada's foray into the battle against money laundering is somewhat similar to that of its southern neighbor. In 1989, following high-level international discussions about the threat of money laundering and the growing need for countries to take measures to better face the issue both domestically and internationally, Canada formally made money laundering an offence under its criminal code (Standing Senate Committee on Trade and Commerce, 2013). Following the passing of this legislation, the Office of the Superintendent of Financial Institutions began to issue guidelines and best practices to combat money laundering, followed soon after by the establishment of Integrated Proceeds of Crime units by the Royal Canadian Mounted Police (RCMP) to allow the organization to conduct investigations relating specifically to money laundering (Standing Senate Committee on Trade and Commerce, 2013).

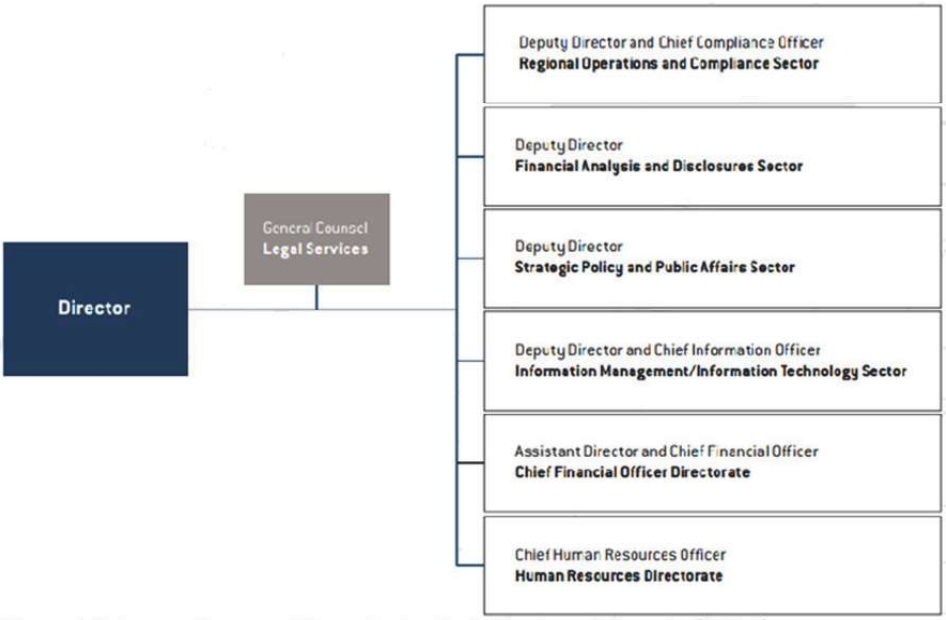
In their original form, Canada's requirements regarding money laundering extended solely to transactions conducted by financial institutions. Its regime required such institutions to record transactions of $10,000 or more, to undertake procedures to identify clients, and to be vigilant for suspicious activities and to report these to the RCMP directly on a voluntary basis (Standing Senate Committee on Trade and Commerce, 2013). This remained the case for approximately ten years, until the regime was investigated and overhauled in 2000.

Financial Transactions and Reports Analysis Centre of Canada

Canada recognized the need to change its anti-money laundering regime in 2000 following a set of recommendations drafted by the Financial Action Task Force (FATF), an international effort to combat money laundering at a global level. These recommendations noted the increasingly global nature of both organized crime and money laundering, as well as the existing limitations in the Canadian regime (Standing Senate Committee on Trade and Commerce, 2013). In response, parliament adopted the Proceeds of Crime (Money Laundering) Act (PCMLA), creating a system for reporting financial transactions considered to be suspicious, large cross-border transfers of monetary instruments, and prescribed transactions considered to be noteworthy, and making reporting on such items mandatory (Capra International Inc., 2010).

During this time, the Federal Government also launched its National Initiative to Combat Money Laundering (NICML), showing its dedication to increasing its focus on money laundering and related activities. Following the September 11, 2001 attacks, Canada, like many of its allied countries, recognized the need to stop financial crimes that may be related to terrorist financing, and NCIML's scope was expanded to what is now called Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime (the Regime). The Regime is the ultimate responsibility of Canada's Department of Finance, with collaboration from a number of other governmental organizations. These groups work together to share information on money laundering, largely through Canada's Financial Intelligence Unit (FIU) the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC's organizational structure includes a Director with overall responsibility for fulfilment of the organization's mandate, and is organized with a series of deputy directors each with a specific area of responsibility. This structure is displayed in Figure 4: FINTRAC Organizational Structure.

FIGURE 4
FINTRAC ORGANIZATIONAL STRUCTURE



Financial Transactions and Reports Analysis Centre of Canada (2014)

FINTRAC's mandate is laid out in the PCMLA. Like FinCEN, its United States counterpart, and other FIUs throughout the world, FINTRAC is tasked with collecting and analyzing financial transaction information for the detection, arrest and prosecution of individuals and groups involved with Money Laundering and Terrorist Financing activities. FINTRAC works with several Canadian enforcement agencies, including (Capra International Inc., 2010).

- **The Royal Canadian Mounted Police (RCMP)**, and in particular its Money Laundering Units (MIUs), which are major recipients of suspected Money Laundering intelligence from FINTRAC, and who are responsible for investigating, laying charges, seizing assets and assisting prosecutions of individuals suspected of Money Laundering or Terrorist Financing.
- **The Canada Border Services Agency (CBSA)**, which is responsible for ensuring that anyone entering or exiting the country with cash or monetary instruments in excess of $10,000 files a proper report so that the transfer can be tracked. Though there is no per se limit on the amount of money an organization or individual may import to or export from Canada, failure to declare such funds can be penalized with seizure and fines. If the funds are believed to be the proceeds of crime or intended to finance terrorist activities, the funds are forfeited with no terms of release. Information on reports and seizures is transferred to FINTRAC, which collects the data and distributes it to appropriate law enforcement agencies.
- **The Canada Revenue Agency (CRA)**, which administers the Income Tax and Excise Tax Acts, which prohibit evasion of taxes. As tax evasion is often involved in Money Laundering or Terrorist Financing activities, co-operation between the CRA and FINTRAC is a key component of the fight against such activities. FINTRAC sends disclosures to the CRA's Enforcement and Disclosures Directorate when its analysis suggests that the information may be linked to a tax or duty evasion offence.

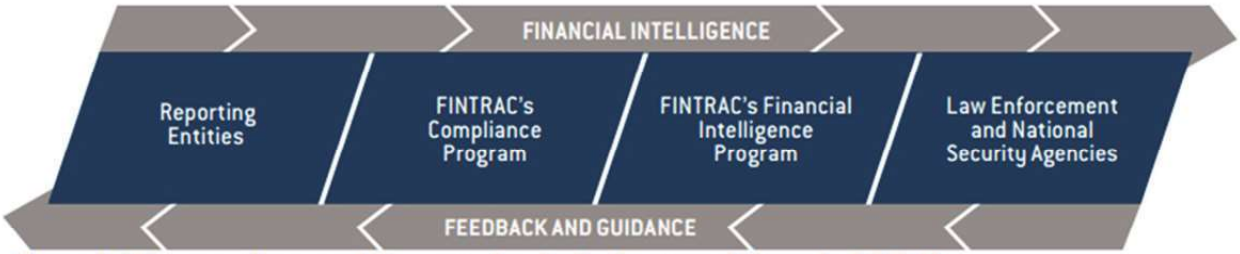
- **The Canadian Security Intelligence Service (CSIS)**, which is responsible for collection, analysis and reporting of intelligence related to Canadian national security. CSIS and FINTRAC share information in the form of reports and disclosures believed to relate to activities that constitute a threat to national security. CSIS also shares such information with other agencies such as the RCMP to aid their efforts in investigating and prosecuting domestic crimes.

In fulfilment of its obligations to Canada's Anti-Money Laundering Efforts, FINTRAC receives reports of specific operations and activities from a set of prescribed entities, commonly referred to as mandatory reporting entities. Such entities include the institutions designated as banks under Schedule I or II of the Bank Act, money services companies, casinos, dealers of precious metals and stones, and securities dealers (Financial Transactions and Reports Analysis Centre of Canada, 2011). The primary documents collected by FINCEN include: Large Cash Transaction Reports (LCTRs), which must be submitted when a prescribed entity receives in excess of $10,000 in cash within 24 consecutive hours from a single individual or organization; Electronic Funds Transfer Reports (EFTRs), which much be submitted when such entities process transfers of over $10,000 into or out of Canada within 24 consecutive hours by a single individual or organization; Suspicious Transaction Report (STR), which entities must submit where they observe suspicious or potentially suspicious activities, and Casino Disbursement Reports, which must be submitted by a casino when it disburses $10,000 or more to a single individual or entity within a 24-hour period. In addition to the reports received from the prescribed entities, FINTRAC also receives two types of reports from the CBSA. The first report, called the Cross-border Currency Report, is filed with the CBSA by a person entering or leaving Canada with cash or monetary instruments of $10,000 or more, or who intend to send sums of such amounts into or out of Canada. The second type of report, the Cross-Border Seizure Report, is submitted when cash or monetary instruments are seized by CBSA due to failure of a traveller to meet reporting obligations.

As in the United States and other countries with strict regulations, Canada's regime places significant onus on mandatory reporting entities to detect and report suspicious activities, levying significant penalties and sanctions against entities showing patterns of non-compliance. Entities are required not only to submit prescribed reports as circumstances require, but to undergo continual training so that staff understand suspicious activities, meet with FINTRAC representatives for compliance meetings, follow up on non-compliance issues or incidents, and submit to compliance examinations administered by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada, 2014). Compliance examinations are considered particularly crucial to FINTRAC, comprising a significant piece of its compliance process. For the 2013-2014 year, the organization verified compliance across institutions by conducting approximately 1,126 compliance examinations throughout Canada (Financial Transactions and Reports Analysis Centre of Canada, 2014).

Within Canada's Anti-Money Laundering and Terrorist Financing Regime, FINTRAC serves a critical central role in collecting, aggregating and disclosing data to appropriate parties, thereby facilitating the transfer of information to ensure law enforcement officials get a clear, concise and timely picture of suspicious activities. The organization also receives information from such agencies, which it uses to give feedback to reporting entities in order to allow them to remain educated about potentially suspicious activities. A diagram of the flow of information to and from FINTRAC is shown in Figure 5: FINTRAC Intelligence and Feedback.

FIGURE 1
FINTRAC INTELLEGENCE AND FEEDBACK



Financial Transactions and Reports Analysis Centre of Canada (2014)

The top side of the diagram shows FINTRAC's receipt of reports from mandatory reporting entities and the CBSA, and disclosure of information derived from these reports to appropriate law enforcement and security agencies. The bottom side shows the back channel of information, where FINTRAC receives feedback on its information collection methods and required compliance from the appropriate agencies or legislative bodies and uses such feedback to improve its own operations and offer guidance to mandated entities and individuals.

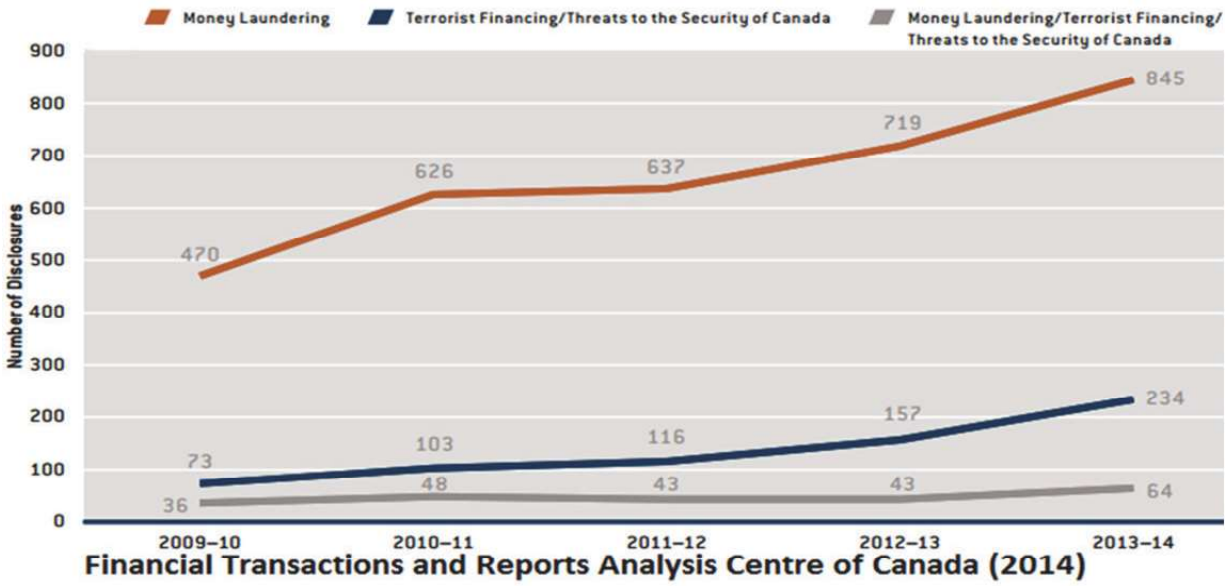
FINTRAC receives an excessive and increasing number of reports each year for analysis and summarization. For the 2011-2012, 2012-2013 and 2013-2014 years, the organization received 18,528,922, 19,744,923 and 19,750,453 reports respectively (Financial Transactions and Reports Analysis Centre of Canada, 2014), broken down as in Table 1: FINTRAC Reports by Type. This table shows the overall increase in total reports, as well as fluctuations in the numbers of specific reports. Of particular note are STRs, which saw a significant increase of approximately 16% from the 2011-2012 to 2013-2014 years. This suggests an increase in either suspicious activities by clients of mandatory reporting entities or the vigilance of such entities in designating client activities as suspicious and making the appropriate reports to FINTRAC.

TABLE 1
FINTRAC REPORTS BY TYPE

Report Type	2011-2012	2012-2013	2013-2014
Large Cash Transaction Reports	8,062,689	8,523,416	8,313,098
Electronic Funds Transfer Reports	10,251,643	10,993,457	11,182,829
Suspicious Transaction Reports	70,392	79,294	81,735
Cross-Border Currency Reports / Cross-Border Seizure Reports	35,026	31,826	42,650
Casino Disbursement Reports	109,172	116,930	130,141
Total	**18,528,922**	**19,744,923**	**19,750,453**

Once collected, FINTRAC is tasked with disclosing in a timely manner reports that may be relevant to financial investigations to the appropriate authorities. Per the organization's 2014 report, the FINTRAC made 1,143 disclosures to its regime partners in the 2013-2014 year, relating to Money Laundering, Terrorist Financing/Security Threats, or both areas. The breakdown of disclosures by category is shown in Figure 6: FINTRAC Disclosures by Category 2009-2014.

FIGURE 2
FINTRAC DISCLOSURES BY CATEGORY 2010-2014



Of the disclosures made to partners, the RCMP and CSIS received the largest share: 703 and 243 disclosures respectively. This is not surprising considering the categorization of disclosures, as these are areas for which those entities are primarily involved in investigations. The predicate offences, as noted in Table 2: Disclosure Predicate Offences, also support the breakdown, as the predicate offences noted as being most prevalent, drug dealing and fraud, are largely handled by the RCMP or CSIS.

TABLE 2
DISCLOSURE PREDICATE OFFENCES

PREDICATE OFFENCE CATEGORY	2011–12	2012–13	2013–14
Drugs	27%	27%	33%
Fraud	35%	34%	28%
Unknown	11%	8%	11%
Tax Evasion	9%	13%	9%
Corruption	5%	5%	5%
Customs/Excise	5%	4%	5%
Theft	6%	5%	5%
Human Smuggling/Trafficking	3%	3%	3%
Illegal Gambling	1%	2%	1%

Source: Financial Transaction and Reports Analysis Centre (2014)

Though praised by law enforcement partners for its assistance in tracking important financial activities, FINCEN and the legislation which led to its creation are not without critics. In particular, the Standing Senate Committee on Banking Trade and Commerce (2013) noted serious concerns with balancing the regime's sharing of information with domestic and international partners against privacy rights guaranteed to Canadian citizens. The Committee also raised concerns with the regime's value-for-

money, noting a lack of information on results and costs of regime investigations. Such comments are not unique to the Canadian environment and are in fact common concerns for anti-money laundering regimes throughout the world.

INTERNATIONAL ANTI-MONEY LAUNDERING EFFORTS

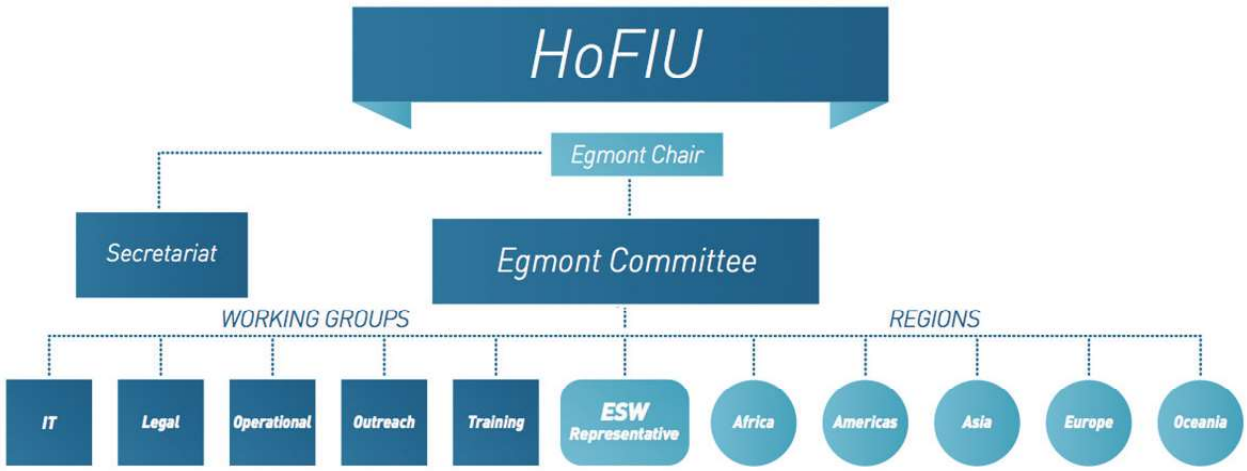
Money laundering, as well as its predicate crimes, often transcends or exploits international borders, allowing criminals to exploit blind spots and deficiencies in communications and enforcement efforts between international actors. To combat this issue, many countries have chosen to work together, allowing them to pool resources and information so that they might better detect, obstruct and punish the practice of money laundering. Two primary institutions stand out in their co-ordination of anti-money laundering efforts across nations. These are the Egmont Group and the Financial Action Task Force (FATF).

Egmont Group

The Egmont group was formed in 1995 when representatives from a small group of concerned countries met in Arbenberg palace in Brussels, Belgium. The group was formed as an informal association of individual countries to combat money laundering domestically, with the goal of fostering international co-operation (Egmont Group, 2004). The Egmont Group helps facilitate the rapid exchange of information based on mutual agreements for information sharing between individual Financial Information Units (FIUs), which it defines as national centres for the "receipt and analysis of (a) suspicious transaction reports; and (b) other information related to money laundering, associated predicate offences and financing terrorism, and for the dissemination of the results for analysis" (Egmont Group, 2015). Examples of North American FIUs include the American FinCEN and Canada's FINTRAC, which were discussed in detail above. From an initial group of approximately 20 countries, Egmont now connects approximately 139 FIUs from countries on every permanently inhabited continent, with expectations of further growth in coming years (Egmont Group, 2013). This increase in membership is reflective of the organization's commitment to assist countries in establishing and supporting FIUs domestically, providing active assistance to countries unable to support their own FIUs. This assistance includes major outreach projects to governments of Africa and Oceania, where special assistance was required to provide proper training and establish frameworks to detect and obstruct money laundering (Egmont Group, 2013).The Egmont group extends the possibility of membership to any FIU that is found to be in compliance with the Group's criteria for membership. The application process is rigorous, involving sponsorship from one or more existing members, a series of onsite visits by Egmont Group officers, and ultimately endorsement by the heads of member FIUs.

FIUs counted as members of the Egmont Group have access to a wealth of data from diverse and reliable sources all over the world. The group is also actively engaged in self-improvement, making its processes and those of its members more accurate, secure, efficient and cost effective. To achieve this goal, the Egmont Group has formed several working groups, each with a mandate to address problems or implement ideas in a specific area. These include the Training Working Group, Outreach Working Group, Legal Working Group, IT Working Group, and Operational Working Group. In addition to these groups, Egmont has also established committees based on region, including Africa, the Americas, Asia, Europe and Oceania. A diagram of the organization's layout is shown in Figure 7: Egmont Group Organizational Structure.

FIGURE 3
EGMONT GROUP ORGANIZATIONAL STRUCTURE



(Egmont Group, 2014)

In addition to its work throughout the world in establishing and supporting FIUs, the Egmont Group has also established ties with other international organizations dedicated to the oversight of international monetary systems and the detection and impediment of money laundering. The most prominent and influential of these is the Financial Action Task Force (FATF), an organization that has shaped and enforced international anti-money laundering policies for over two decades.

Financial Action Task Force

In the late 1980s, the same concerns over the impact of money laundering that prompted the United States and Canada to draft specific legislation to combat the practice and establish their own FIUs led the member nations of the G7 to establish the Financial Action Task Force (FATF). Founded in 1989, this inter-governmental body is responsible for examining prevailing trends and methods used to launder money, reviewing initiatives in place by individual countries and the international community, and developing and augmenting anti-money laundering measures to ensure peak effectiveness. The initial representation of the G7 countries has grown substantially in the years since the establishment of the FATF. Today, the group has a total membership of 36, with several regional entities based on its model that enjoy the status of designated observers of the group's regulations (Financial Action Task Force, 2012).

The FATF's role in combating international money laundering cannot be overstated. It was this organization's findings and sanctions, laid out in its Forty Recommendations, first released in 1990. These recommendations included a broad set of measures to allow individual countries to identify, obstruct, and reprimand money laundering as well as other instances of criminal exploitation of financial systems (Financial Action Task Force, 2014). Understanding that money laundering is a continually evolving process, with criminals constantly testing limits and searching for loopholes or regime weaknesses to allow them to escape prosecution, the FATF was established without a restrictive constitution and without a definite lifespan. The group evaluates its own mandate and methods regularly and adjusts these as necessary to reflect the current state of money laundering, as well as world events that might impact the organization's scope. The FATF's mandate is updated every few years, with its current mandate established in 2012 and in place until 2020 (Financial Action Task Force, 2014).

As the methods of exploitation employed by financial criminals has grown and expanded, so too have the recommendations produced by the FATF. In response to the September 11, 2001 terror attacks, the FATF recognized the significant threat of the financial system being used to facilitate terrorist financing, and its scope was expanded to include the obstruction of terrorist financing. This was followed by the

group's publishing of 9 Special Recommendations on Terrorist Financing, intended to give member FIUs guidance as they developed their individual Anti-Terrorist Financing regimes. These too continue to evolve as the FATF receives new information and arrives at new methods to combat terrorist financing.

As is the case with the Egmont Group, the FATF has a rigorous process for attaining membership, ensuring that potential members can obey the organization's strict rules and regulations. Prospective members must meet a list of criteria that are both fundamental and technical in nature to be considered for full membership. These include commitment to AML/CFT efforts, observance of financial sector standards, and ratification of Financial Action Task Force Recommendations with agreement to fully adopt the recommendations within three years (Financial Action Task Force, 2012). FATF jurisdiction and organizations commit to endorse and implement its recommendations and submit to peer review and follow-up processes to keep their regimes in compliance (Financial Action Task Force, 2012). The FATF also considers compatibility criteria such as the jurisdiction's gross domestic product (GDP) and its overall impact on the global financial system (Financial Action Task Force, 2014b).

To best address the issues of money laundering and terrorist financing, the FATF has organized itself into working groups, each responsible for specific tasks contributing to the group's overall functionality. These primarily include (Financial Action Task Force, 2009):

- **the Working Group on Typologies**, tasked with identifying and monitoring emerging trends in money laundering and terrorist financing;
- **the Working Group on Terrorist Financing and Money Laundering**, responsible for developing and interpreting guidance on existing standards as well as novel and emergent issues;
- **the Working Group on Evaluations and Implementation**, which also interprets and develops guidance on the standards, as well as co-ordinating, monitoring and reviewing evaluation processes and procedures for member organizations; and
- **the International Co-operation Review Group**, which is charged with examining jurisdictions that fail to implement effective Anti-Money Laundering or Terrorist Financing measures, and recommend improvements where required.

The FATF plays a critical role in maintaining oversight and facilitating co-operation and exchange of information between member countries throughout the world. Its recommendations have offered critical guidance to FIUs in enhancing their individual programs and working toward information-sharing and co-operation with the common goal of combating threats common to the global financial system. The organization continues to shape the course of AML/CTF efforts throughout the world, self-assessing, self-correcting, and self-regulating its methods and scope as it develops and as the needs of the global financial system change.

CONCLUSION

Despite their detractors, who primarily question either the efficacy of AML policies or the balance between enforcement of financial legislation and the rights of common citizens to privacy and the benefit of the doubt, the Anti-Money Laundering efforts of Canada, the United States, and the world continue to advance. Though there are no doubt valid questions regarding the inner workings of information-sharing programs domestically and internationally, the organizations involved have taken great strides to ensure co-operation and take actions to combat financial crimes.

Domestically, the efforts of FINTRAC remain invaluable for collecting, analyzing and acting upon information derived from reporting entities so that aggregated data can help inform the decisions and actions of the proper authorities. Likewise, the organization acts as a facilitator of transfer of feedback and current trends from enforcement agencies to reporting entities, so that they may remain aware of salient threats of which they become aware. This mandate gives FINTRAC and the AML Regime in Canada an incredibly important task in defending the country's financial system from criminals who would exploit it, whether following or in advance of illicit activities.

Even as international syndicates of criminals and anarchists search for new ways to obviate the protections inherent in the existing financial system and avoid reporting income, paying taxes or drawing attention to their illicit activities, law enforcement groups throughout the world are gathering and sharing information on an unprecedented scale to obstruct such activities and maintain the integrity of domestic and international financial systems. Though these groups move more slowly than their criminal counterparts, their increasing sophistication, internal transparency, and commitment to good governance and oversight give them an advantage in their war against money laundering and its predicate crimes.

REFERENCES

107th Congress of the United States of America. (2001, October 24). *USA PATRIOT Act (H.R. 3162)*. Retrieved March 15, 2015, from Enforcement Policy Information Center: https://epic.org/privacy/terrorism/hr3162.html

Balko, R. (2014, March 24). *The federal 'structuring' laws are smurfin' ridiculous*. Retrieved March 5, 2015, from The Washington Post Online: http://www.washingtonpost.com/news/the-watch/wp/2014/03/24/the-federal-structuring-laws-are-smurfin-ridiculous/

Business Crime Solutions Inc. (n.d.). *Money Laundering: A Three-Stage Process*. Retrieved March 5, 2015, from Business Crime Solutions: https://www.moneylaundering.ca/public/law/3_stages_ML.php

Capra International Inc. (2010, December 7). *10-Year Evaluation of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*. Retrieved February 12, 2015, from Department of Finance Canada: http://www.fin.gc.ca/treas/evaluations/amlatfr-rclcrpcfat-eng.pdf

Duhaime Law. (2015). *Prepaid Access*. Retrieved March 5, 2015, from Duhaime's Anti-Money Laundering Law in Canada: http://www.antimoneylaunderinglaw.com/emerging-trends/prepaid-access

Egmont Group. (2004, September). *Information Paper on Financial Intelligence Units and the Egmont Group*. Retrieved March 26, 2015, from Egmont Group: http://www.egmontgroup.org/library/egmont-documents

Egmont Group. (2013). *About*. Retrieved March 27, 2015, from The Egmont Group of Financial Intelligence Units: http://www.egmontgroup.org/about

Egmont Group. (2014). *Structure and Organization of the Egmont Group of Financial Intelligence Units*. Retrieved April 4, 2015, from The Egmont Group of Financial Intelligence Units: http://www.egmontgroup.org/about/structure-and-organization-of-the-egmont-group-of-financial

Egmont Group. (2015). *Financial Intelligence Units (FIUs)*. Retrieved March 18, 2015, from Egmont Group: http://www.egmontgroup.org/about/financial-intelligence-units-fius

Egmont Group Secretariat. (2013). *Egmont Group of Financial Intellligence Units Annual Report 2012-2013*. Retrieved March 31, 2015, from The Egmont Group of Financial Intelligence Units: http://www.egmontgroup.org/library/annual-reports

Financial Action Task Force. (2009). *Financial Action Task Force Annual Report*. Retrieved March 12, 2015, from Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/2008%202009%20ENG.pdf

Financial Action Task Force. (2012, April 20). *Financial Action Task Force Mandate (2012-2020)*. Retrieved April 2, 2015, from Financial Action Task Force Website: http://www.fatf-gafi.org/media/fatf/documents/FINAL%20FATF%20MANDATE%202012-2020.pdf

Financial Action Task Force. (2013, June). *Prepaid Cards, Mobile Payments and Internet-Based Payment Services*. Retrieved February 22, 2015, from Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf

Financial Action Task Force. (2014, October 22). *FATF 40 Recommendations*. Retrieved March 29, 2015, from Financial Monitoring Unit: http://www.fmu.gov.pk/docs/FATF_40Recommendations.pdf

Financial Action Task Force. (2014, June). *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Retrieved March 12, 2015, from Financial Action Task Forrce: http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Financial Action Task Force. (2014b). *FATF Membership Policy*. Retrieved April 3, 2015, from Financial Action Task Force: http://www.fatf-gafi.org/pages/aboutus/membersandobservers/fatfmembershippolicy.html

Financial Crimes Enforcement Network. (2005). *Reporting Suspicious Activity*. Retrieved February 23, 2015, from Financial Crimes Enforcement Network: http://www.fincen.gov/statutes_regs/guidance/pdf/msbsar_quickrefguide.pdf

Financial Crimes Enforcement Network. (2011, December). *FinCen Annual Report Fiscal Year 2011*. Retrieved March 5, 2015, from Financial Crimes Enforcement Network: http://www.fincen.gov/news_room/rp/files/annual_report_fy2011.pdf

Financial Crimes Enforcement Network. (2012). *FinCEN - Our Story*. Retrieved February 15, 2015, from Financial Crimes Enforcement Network: http://www.fincen.gov/about_fincen/pdf/OverallChart.pdf

Financial Crimes Enforcement Network. (2013). *FinCEN's Mandate From Congress*. Retrieved March 2, 2015, from Financial Crimes Enforcement Network: http://www.fincen.gov/statutes_regs/bsa/

Financial Crimes Enforcement Network. (2014, May). *Bank Secrecy Act Timeline*. Retrieved February 18, 2015, from Financial Crimes Enforcement Network: http://www.fincen.gov/statutes_regs/bsa/bsa_timeline.html

Financial Crimes Enforcement Network. (2015, March 31). *FinCEN's 314(a) Fact Sheet*. Retrieved March 31, 2015, from Financial Crimes Enforcement Network: http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf

Financial Transactions and Reports Analysis Centre of Canada. (2011, December 11). *Who must report*. Retrieved from Financial Transactions and Reports Analysis Centre of Canada: http://www.fintrac.gc.ca/reporting-declaration/Info/re-ed-eng.asp

Financial Transactions and Reports Analysis Centre of Canada. (2014). *Deter and Detect: Money Laundering and Terrorist Financing FINCEN Annual Report 2014*. Retrieved March 15, 2015, from Financial Transactions and Reports Analysis Centre of Canada: http://www.fintrac.gc.ca/publications/ar/2014/ar2014-eng.pdf

Government Accountability Office. (2010, April 28). *FinCEN Needs to Further Develop Its Form Revision Process for Suspicious Activity Reports*. Retrieved from Government Accountability Office: http://www.gao.gov/assets/130/124551.pdf

Gray, J. (2014, December 23). *Not Just a Stocking Stuffer: Gift Cards A Money-Laundering Loophole*. Retrieved January 12, 2015, from The Globe and Mail: http://www.theglobeandmail.com/report-on-business/not-just-a-stocking-stuffer-gift-cards-a-money-laundering-loophole/article22194461/

Groenfeldt, T. (2014, April 16). *Prepaid Cards to Hit $200 Billion in Merchant Sales in 2014*. Retrieved April 3, 2015, from Forbes: http://www.forbes.com/sites/tomgroenfeldt/2014/04/16/prepaid-cards-to-hit-200-billion-in-merchant-sales-in-2012/

Internal Revenue Service. (2015, February 4). *Overview - Money Laundering*. Retrieved March 3, 2015, from Internal Revenue Service Website: http://www.irs.gov/uac/Overview---Money-Laundering

Internal Revenue Services. (2015, February 15). *Examples of Money Laundering Investigations - Fiscal Year 2015*. Retrieved March 12, 2015, from Internal Revenue Service: http://www.irs.gov/uac/Examples-of-Money-Laundering-Investigations-Fiscal-Year-2015

International Money Laundering Information Bureau. (2015, January 16). *Money Laundering - What Is Money Laundering?* Retrieved January 29, 2015, from International Money Laundering Information Bureau: http://www.imlib.org/page2_wisml.html

Matonis, J. (2013, May 7). *The Monetary Future*. Retrieved February 20, 2015, from American Banker: http://www.americanbanker.com/bankthink/money-laundering-is-financial-thoughtcrime-1058902-1.html?zkPrintable=1&nopagination=1

Reuter, P. A. (2004). *Chasing Dirty Money: The Fight Against Money Laundering*. Retrieved from http://www.piie.com/publications/chapters_preview/381/1iie3705.pdf

Standing Senate Committee on Trade and Commerce. (2013, March). *Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing?* Retrieved March 10, 2015, from Parliment of Canada Website: http://www.parl.gc.ca/Content/SEN/Committee/411/BANC/rep/rep10mar13-e.pdf

U.S. Department of the Treasury. (2013, June 28). *Bureaus*. Retrieved February 27, 2015, from U.S. Department of the Treasury: http://www.treasury.gov/about/organizational-structure/bureaus/Pages/default.aspx

United States Government Accountability Office. (2014, May). *Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*. Retrieved March 20, 2015, from United States Government Accountability Office: http://www.gao.gov/assets/670/663678.pdf

Velde, F. (2013, December). Bitcoin: A Primer. *Chicago Fed letter,* (317), pp. 4-7.