LexisNexis® Emerging Issues Analysis

Jeffrey Simser on

Money Laundering: Predicate Crimes, Laundering Techniques and the AML Response

2012 Emerging Issues 6195

Click here for more Emerging Issues Analyses related to this Area of Law.

The acquisition of, and control over, wealth is the motivation for most serious crimes involving premeditation.[1]

Money laundering or ML is a technique used to disguise the origin of tainted property, shielding that property from law enforcement, victims and criminal predators. Estimates suggest that global ML involves between $500 billion and $1 trillion a year. One commentator has suggested that the most authoritative estimate is a decade old and has a $1 trillion deviation between the high and low end of the scale.[2] In my country, Canada, between $5 billion and $15 billion (Cdn) is estimated to be laundered annually.[3] We clearly lack an accurately quantified understanding of ML. This isn't surprising. A truly successful money launderer is a covert figure hoping never to be discovered. Laundered money is not meant to be counted by financial institutions, authorities or statisticians. We know, through typologies, prosecutions and financial intelligence unit analysis, that ML is a serious problem which governments and international bodies have grappled with for the past twenty-five years. An industry devoted to anti-money laundering or AML efforts has resulted.[4] AML efforts are targeted at conventional laundered money (drug proceeds, for example) as well as countering the financing of terrorism (CFT) efforts. This paper focuses primarily in two areas: the predicate crimes that lead to ML and the techniques that launderers use. In concluding, the paper takes a brief look at AML systems and the consequent enforcement mechanisms to deal with ML.

What is Money Laundering?. Canada's financial intelligence unit defines money laundering as:

> "the process whereby "dirty money", produced through criminal activity, is transformed into 'clean money' whose criminal origin is difficult to trace.

---

1 Rider, B *Recovering the Proceeds of Corruption* (2007), 10 J Money Laundering Control 5 at 9.
2 Demetis, D *Unfolding Dimensions of an Anti-Money Laundering/Counter-Terrorist Financing Complex System* (October, 2011: LexisNexis Emerging Issues Analysis 6019) at p. 12.
3 Brennan, S; Vaillancourt, R *Money Laundering in Canada, 2009* (Ottawa: Statistics Canada, Juristate Bulletin Article 85-005-X, June 21, 2011) at p.1.
4 The *Money Laundering Control Act* was passed by the U.S. Congress in 1986 and is codified at 18 USC §§ 1956-1957 (2000) and 31 USC §§ 5324-5326 (2000).

> Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention."[5]

Generally, money laundering is thought to have three steps: one, money enters the financial system, a step often referred to as placement (sometimes called loading); the launderer then takes steps, commonly known as layering, to obfuscate the source of the money; finally the apparently cleansed money is organized under the patina of legitimacy, a step known as integration. As we shall see, these steps are not always followed or even present. A fraudster will often take victim money from within the financial system and has no need to worry about the placement step; by way of contrast, a drug dealer runs a cash business and placement is a critical ML step.

A hypothetical money laundering transaction might begin with the sale of illegal drugs. Let's say a dealer sells cocaine in Toronto for $100,000. The buyer deals with street transactions and gets paid in cash. So our hypothetical dealer now has $100,000, likely in lower denomination bills. The dealer could retain a few trusted associates and instruct them to make bank deposits, all of which will be under $10,000, into various institutions. Ideally our dealer may have set up a sham (or a real) cash business like a restaurant or a Laundromat, to facilitate the deposits. The drug dealer then moves the money from those accounts into others, hoping to hide his tracks. There are lots of techniques available to our dealer. The dealer could cut a cheque from an account in the name of his "cash" business to ostensibly settle an invoice from a shell company in his or her control. Once the dealer is satisfied that the money trail has been appropriately obscured, the money can be moved back to his own Toronto account; that $100,000 in cocaine wealth now has the patina of a legitimate provenance. Our drug dealer now presents to the community as a legitimate businessperson. As we shall see, money laundering techniques are limited only by the imagination.

Money laundering is, in and of itself, a crime. In Canada:

> Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of

---

5 http://www.fintrac.gc.ca/questions/FAQ/faq_question-eng.asp?CatID=61&ID=161&Ord=1 last viewed on October 14, 2011.

> (*a*) the commission in Canada of a designated offence; or
>
> (*b*) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence.[6]

The offence is defined in fairly broad terms, although its scope is limited to designated offences, which are essentially offences that may be prosecuted as an indictable offence.[7] There are professional launderers who will take a percentage of the cash to load illicit cash into the system.[8] In many instances, if not the majority, criminals self-launder. They may involve associates or family members, but they are either unwilling or lack the wherewithal to give up seven or eight points on their ill-gotten gains top a professional launderer.[9] In the case of self-laundering, there are two potential offences to look at: the initial or predicate crime (drugs, fraud and so on); then the subsequent crime of money laundering.

Terrorist Financing

In addition to money laundering, our AML systems have been tasked with combating or countering the financing of terrorism, sometimes known as CFT work.[10] This is a counter-intuitive form of money laundering. Normally ML involves tainted funds that are meant to be cleansed and often intended to be used for more or less legitimate purposes (buying a luxury home, for example). Terrorist financing money often has a legitimate provenance, like a charitable donation, which is then converted for the most nefarious of purposes, a terrorist attack. The amounts of money in CFT cases are comparatively small. Significant terrorist events can cost as little as $10,000 to $15,000. Even the notorious events of 9/11 cost less than $500,000. The motivation for ML, greed, is generally not present in terrorist financing (although it can be).[11] Money launderers tend to return to the predicate activity that made money for them (drugs,

---

6 See s. 462.31 of the *Criminal Code*, R.S.C. 1985 C-c.46 (the "Code").

7 Section 462.3 of the Code defines designated offences, which also include conspiracy, attempt to commit, accessory after the fact or counseling. There are also certain offences excluded by regulation, see: Regulations Excluding Certain Indictable Offences from the Definition of "Designated Offence", SOR/2002-63.

8 There's an interesting discussion on the historic differences between Canadian and American approaches (although Canadian law has since changed) as well as to the role of a professional launderer in *United States of America v. Dynar*, [1997] 2 SCR 462.

9 That was the spread in *R. v. Rosenfeld*, 2009 ONCA 307 (CanLII) where a lawyer was convicted of money laundering; a police officer, posing as a front man for a Columbian drug cartel, retained the defendant and both sides agreed to an 8 percent fee for laundering money.

10 Also known as CTF or countering terrorism financing.

11 Many terrorist organizations that fail to achieve their ends continue on in the interests of self-preservation and become, in essence, continuing criminal organizations. Examples range from the mafia, formed to expel Napoleon from Italy, through to many modern triads. See Rider, B *Recovering the Proceeds of Corruption* (2007), 10 J Money Laundering Control 5 at 14.

fraud and so on) whereas terrorists tend to commit singular acts. That singularity makes detection even more difficult; there's no pattern to sift through.[12]

Predicate Crimes and ML Risk. While ML is, in and of itself, a crime, generally there's another crime (drugs, fraud and so on) informing and modifying the ML. I call these offences "predicate" crime. Modern AML systems take a risk-based approach, something discussed in detail later in this paper. Properly understood, ML risk is largely informed by the predicate crimes that create the tainted wealth being laundered. Predicate crimes like drug trafficking pose a high risk at the placement or cash loading stage. Street sales of drugs are conducted in cash. Other predicates like fraud, pose different ML risks. The victim is often within the financial system itself and may, for example, write a cheque to the fraudster. The fraudster doesn't have the cash problem that the drug dealer does and their ML activity tends to operate at the layering and structuring stages. Both a drug dealer and fraudster pose AML risk to a financial institution. The fraudster poses an additional risk: fraudsters love to scam financial institutions and include them in their list of victims. This next section delves into the predicate crimes that lead to money laundering and the discussion is by no means a complete one, rather the intent is to discus some significant and some intriguing predicate crimes that inform AML risk.

Drugs

210 million people consume illicit drugs each year and almost 200,000 die annually.[13] The global retail market for cocaine is estimated to be worth $88 billion and the opiate retail market is worth $65 billion. By volume, cannabis is the largest illicit drug and the market for amphetamine-type stimulants is comparable to the heroin market. By contrast, trafficking in persons garners $32 billion and firearms a mere $1 billion.[14] Drug trafficking at the retail level is a cash business. Street dealers exchange drugs for $10 and $20 bills. That money poses a number of risks from the drug dealer's perspective. There is the risk that other members of the criminal fraternity will attack and rob the drug dealer of their money. There is the risk of exposure to law enforcement: cash, compared to drugs like cocaine, is bulky. Street and middle level drug dealers need to "load" their cash into the financial system, a technique generally referred to as placement. Larger scale drug trafficking organizations use virtually every known ML technique (and likely others not yet discovered). Drugs are the ultimate predicate crime.

---

12 Simser, J *Terrorism Financing and the Threat to Financial Institutions* (2011), 14 J Money Laundering Control 334.
13 United Nations Office of Drugs and Crime *World Drug Report 2011* (Vienna: UNODC, 2011) p. 8.
14 Ibid at p. 33.

Consider, for example, the cocaine market. Columbian drug lord Pablo Escobar muscled into the trade and became a major figure, in the 1970's and 1980's. Initially he collected cash, but as the enterprise grew, his quantities of cash became unmanageable and Pablo engaged his brother, an accountant. His brother operated a large number of bank accounts and encouraged Pablo to invest in real estate. The accountant also created a second set of books for Pablo's real estate holdings: if an apartment was sold for $50,000, the books would record the sale at $90,000. Through this simple method, the Escobars, in their words, "were able to create very complicated paths that were impossible to follow to the source."[15] Columbia, along with Bolivia and Peru, continue to be the source of today's cocaine trade, however Mexican cartels have muscled in and now control 90% of the cocaine that reaches American streets.[16] Those cartels smuggle staggering amounts of cash (between $18 and $39 billion US) across the US Southwest border annually.[17] The cartels move cash from local U.S. drug markets into consolidation areas (Atlanta, Chicago, Los Angeles, New York City and North Carolina) where a cell leader takes the currency over border.[18]

Cannabis is the most used drug type, followed by amphetamine-type stimulants (methamphetamine, amphetamine and ecstasy) and opioids (opium and heroin as well as prescription opioids). New illicit drugs, particularly synthetic compounds, are constantly emerging; for example "spice" is a synthetic cannabinoid. Drugs are a massive global business and a primary source of tainted funds. The Mexican cartels are not only notorious for their appalling use of violence and corrosive application of corruption inside Mexico. They also have significant organizational assets throughout the Americas, West Africa (as a key transit point for trade and increasingly as a market) and Europe. The significant earnings of the cartels are laundered using every conceivable technique (and likely some that are inconceivable). From an AML risk perspective, two features of the drug trade are particularly worth noting: the retail transactions are conducted in cash; drug trafficking organizations are truly global.

Fraud

---

15 Escobar, R (with D Fisher) *The Accountant's Story* (New York: Grand Central Publishing, 2009) p. 26.
16 Simser, J *Plato o Plomo: penetration, the purchase of power and the Mexican drug cartels* (2011), 14 J Money Laundering Control 266 at 269.
17 Stana, R (Director Homeland and Security Issues) *Testimony Before the Senate Caucus on International Narcotics Control* (Washington: Government Accountability Office, March 9, 2011) at p. 1.
18 National Drug Intelligence Centre *National Drug Threat Assessment, 2010* (Washington: Department of Justice, 2010).

A study on "occupational" fraud estimated that annual losses to companies globally could be in the order of $2.9 trillion. Occupational fraud generally refers to fraud committed on an organization by an insider who misappropriates assets, is implicated in corruption or issues fraudulent financial statements.[19] There are countless other types of fraud ranging from massive investment schemes, sometimes referred to as "Ponzi" schemes,[20] through to phishing and consumer telemarketing and credit card scams. Unlike drug dealers, fraudsters rarely have a cash loading or placement problem. Typically the victim moves money from their account, within the financial system, into the account of the fraudster. The fraud itself is sustained by the patina of legitimacy designed to fool not only their victim but also their financial institution. A fraudster needs to be trusted by those that they lie to.

In the United States, more than 300 insured depository institutions have failed since 2007, incurring costs of $60 billion to the deposit insurance fund.[21] Not co-incidentally, Ponzi schemes failed during this time too, including Bernie Madoff's notorious scam.[22] As markets melted down, liquidity became an issue: people wanted to be in a cash position. This literally created a "run" on the Ponzi funds. Victims wanted out of their high return investment; intuitively, investors equate high return with high risk, although most victims likely didn't understand exactly how high the risk in fact was. For the same reason there was no queue of potential victims. In a Ponzi, here is no "real" business producing spectacular returns. Further, Ponzi schemes need constant influxes of new money; older "investors" are paid out of new "investor" money; word of mouth from older investors, who are after all getting paid, delivers a new group of victims to the fraudster.

In the Stanford Financial Group case, investors bought certificates of deposit with abnormally large returns; there is comparatively little money recovered and available for victims.[23] Victim money travelled through financial institutions to offshore destinations including Europe, Canada and the Caribbean (notably Antigua). In scams, investors are not the only victims. J.P. Morgan Chase is vigorously defending a $19 billion lawsuit

---

19 This number is premised on the estimate that businesses lose 5% of their revenue to fraud: Association of Certified Fraud Examiners *Report to the Nations on Occupational Fraud and Abuse* (Austin: ACFE, 2010) at p.4.

20 In the 1920's, Charles Ponzi induced thousands to invest in his arbitrage program involving European currencies and international reply coupons issued by European governments. In fact new investor money was used to pay returns to current investors. This type of fraud is exposed when the fraudster cannot bring a sufficient number of new investors or when the current investors withdraw in large numbers. Smith, F *Madoff Ponzi Scheme Exposes "The Myth of the Sophisticated Investor"* (2010-2011), 40 U. Balt L Rev 215 at 221-222.

21 Government Accountability Office *Bank Regulation: Modified Prompt Corrective Action Would Improve Effectiveness* (Washington: GAO-11-612, June 2011).

22 An estimated $50 billion went missing; see for example: *In The Matter of Bernard L Madoff*, [2009] EWHC 442 (Ch).

23 Steffy, L *Forensic Accountant Gives Stanford Investors a Little Hope* (Houston: Houston Chronicle, February 27, 2011). See also *Re:Stanford International Bank*, [2010] EWCA Civ 137.

launched by the trustee in the Madoff fraud.[24] Victims often lack the wherewithal to properly identify risk. This is also true of some public institutions. An inspector general report criticized the Securities and Exchange Commission (SEC) finding that they were aware as early as 1997 that Stanford "was likely operating a Ponzi scheme" a mere two years after Stanford registered with the SEC.[25]

From an AML perspective, corporate fraud detection systems within an institution can play a role in identifying this ML risk. Some frauds have particular hallmarks. For example, a consumer level fraud will often be accompanied by significant credit card charge backs. AML compliance failure exposes an institution to regulatory action, even prosecution. In fraud, there is, potentially, another level of exposure; the fraudster is unlikely to leave a satisfactory asset pool for victims; victims will look for anyone in the narrative with deep pockets, a list that can include transacting institutions. Further the fraudster would be perfectly happy to add the institution to the list of their victims.

Terrorism

As noted above, combating or countering the financing of terrorism (CFT) work is counterintuitive. Money laundering is the art of hiding dirty money. CFT involves small sums, often with a legitimate provenance, that are destined to fund horrific ill deeds. CFT work is backstopped by international conventions and domestic legislation.[26] For institutions, there are a few things worth noting:

- One, the typologies around terrorism may be evolving. For example, traditional organized crime hasn't particularly developed a link to terrorism. Organized crime profits from stable societies, governments and a global financial system. Newer forms of organized crime, often emerging from conflict states, may have a different imperative. They have emerged from chaos, exploiting weak states to further their goals. Even if they don't share the agenda of a terrorist organization, newer organized crime groups can profit from the attendant conflict.[27]

---

24 Associated Press *Trustee Appointed to recover funds in Madoff fraud seeks billions more from JP Morgan Chase* (New York: AP, June 25, 2011).
25 U.S. Securities and Exchange Commission Office of the Inspector General *Investigation of the SEC's Response to Concerns Regarding Robert Allan Stanford's Alleged Ponzi Scheme* (Washington: SEC Case No. OIG-526, March 31, 2010) at p.16.
26 See for example: UN Resolutions 1373 and 1390 adopted under the mandatory provisions of the UN Charter; or Canada's *Proceeds of Crime (Money Laundering) and Terrorism Financing Act*, SC 2000, c.17.
27 Perri, F; Brody, R *The dark triad: organized crime, terror and fraud* (2011), 14 J Money Laundering Control 44 at 45-46.

- Two, terrorist groups will exploit any opportunity to raise funds for their cause, be that donations to "charity" or drug sales or fraudulent activity. In other words, an AML system may detect ML activity which is contemporaneously terrorist financing activity as well.[28]

- Three, the preventative design of the AML system is likely keeping some terrorist organizations out of the formal financial system, forcing them to informal systems like a hawala or to other techniques like the smuggling of cash or jewels.

- Four, terrorist groups need financing not just for singular acts, but also to sustain the operations of their organization.[29]

- Finally, if an AML system fails, the cost to the institution could reach far beyond regulatory consequences; this is a field in which the potential reputational risk is huge.

Corruption

Each year between $1 trillion and $1.6 trillion in public assets are stolen; corrupt officials, particularly in developing countries, loot as much as $40 billion a year.[30] In 2006 the President of Nigeria estimated that corruption and kleptocrats cost Africa 25% of its national income, $148 billion a year.[31] To address this problem, a number of countries have criminalized bribery.[32] There are numerous international conventions, including the United Nations Convention Against Corruption.[33]

ML activity can occur on both sides of a corruption transaction. In Canada and elsewhere, companies are strictly prohibited from engaging in bribery at home or more importantly abroad.[34] Someone wishing to evade the consequences of that prohibition could well participate in "laundering" their money to hide the connection between themselves and foreign bribery. In other words, a company may take money with a legitimate provenance, move it to the country where the bribe is to occur and mask its

---

28 See for example a case in which donations collected for the Tamil people, but in fact were collected for the LTTE (the Tamil Tigers): *R. v. Thambaithurai*, 2011 BCCA 137 (CanLII).
29 Simser, J *Terrorism Financing and the Threat to Financial Institutions* (2011), 14 J Money Laundering Control 334 at 335-336.
30 Greenberg,T; Samuel, L; Grant, W; Gray, L *Stolen Asset Recovery* (Washington: World Bank/UNODC, 2009) p. 6.
31 Simser, J *Asset Recovery and Kleptocracy* (2010), 17 J Financial Crime 321 at 322.
32 See for example Britain's *Bribery Act, 2010*, c.23.
33 There's an Inter-American Convention against Corruption and the African Union Convention on Preventing and Combating Corruption: Muzila,L; Morales,M; Mathias,M; Berger,T *Illicit Enrichment* (Washington: World Bank/UNODC, 2011) at p. ix.
34 *Corruption of Foreign Public Officials Act*, SC 1998, c 34.

source to avoid prosecution back home. Naturally the person taking the bribe will also take steps to either make the payment look legitimate or to launder the money and hide it away. The risk can present itself in a different way. If I want my Canadian company to do business in a country where bribery is rampant, I may attempt to sidestep the prohibitions through the use of a third party or agent. I will pay that agent a commission for sales or contracts and be wilfully blind to the methods used by the agent. In the UK, Aon Limited was fined £5.25 million by the Financial Services Authority (FSA) for making suspicious payments totalling $7 million (US) into high risk countries; the essence of the FSA case was Aon's weak control and oversight process.[35]

In larger corruption cases, money may be hidden away, but not integrated. For example, by 1999 Nigeria had lost over $75 billion to corruption, with $65 billion of this transferred abroad and only a tiny percentage recovered.[36] In other words, the money was spent in London and Paris, not Lagos or Abuja. One method that AML systems employ is the identification of PEPs or politically exposed persons.[37] The basic concept is sound: institutions need to be circumspect and very careful when payments are made to individuals who, through their political positions, are susceptible to bribery and corruption. Where an institution truly knows their customer or applies extra due diligence in high risk areas, the lists can be useful. However, the lists have limitations. If I am a PEP, surely I am crafty enough to know that my wealth can be identified and captured if I use my own name, or that of a relative. So I will use the same, simple techniques that every money launderer uses, transfer and misrepresentation, to game the AML system. If I'm good, I'll render the PEP list meaningless.

Piracy

Of late, piracy, particularly in the Gulf of Aden, has dominated headlines around the world. As ransom payments continue to escalate (the record payment of "$2 million for the Sirius Star in 2009 has been exceeded ever since."),[38] people are asking: where is that money going? We know where it comes from: ship owners want their crews back and calculate not only the cost of the payment, but also the costs of their ships not running on a daily charter basis. We have a sense of how pirates deal with the money: roughly one third will pay for operating expenses (guards, bribes, accommodations,

35 FSA, January 8, 2009: FSA Fines Aon Limited: http://www.fsa.gov.uk/pages/Library/Communication/PR/2009/004.shtml (last viewed October 26, 2011).
36 Simser, J *Asset Recovery and Kleptocracy* (2010), 17 J Financial Crime 321 at 322.
37 See for example, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184, (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).
38 Maria Costa, *Assisting Somalia to Deal with its Pirates* (New York: United Nations Office of Drugs and Crime Statement to the General Assembly of the U.N., May 14 ,2010) at p. 2.

food for the crew and so on); at least one fifth will go to the operating minds of the enterprise and the balance will go to individual pirates who are paid on a scale with union-like rules (first on board gets the biggest cut; a pirate may collect $10,000 to $15,000 of the ransom).[39] In May of 2008, the M.V. Victoria was attacked by 8 pirates and held until the following July, when a $1.8 million ransom was paid. A Canadian journalist estimates the ransom was shared as follows: the commander-in-chief and investor got one half, $900,000; the interpreter and accountant each received $60,000; the commander of the khat received $30,000; the first to board got $150,000 (plus a land cruiser) while the other attackers were paid $41,000 each; cooks and holders got between $9,000 and $20,000 for their work.[40] Lesser members of the organization tend to quickly fritter away their money on drugs and four-wheel drive vehicles. The operating mind of the enterprise fronts certain expenses, but no doubt seeks a nest-egg for later use. That's the money that gets laundered and we seem to have a relatively poor handle on where it's going.[41] In 2010, at least 790 crew members were taken hostage and between $180 and $238 million was paid in ransom. While the quantum is small in comparison to drugs, the cost of piracy increases exponentially when one factors the cost of naval escorts and losses to shipping companies. A United Nations Security Council Resolution calls upon nations to investigate international criminal networks responsible for piracy and follow up on money laundering.[42] As part of the solution, the international community needs to help countries like Kenya, Uganda, the Seychelles, Yemen, Ethiopia and Tanzania build their capacity to address money laundering. Additionally, AML systems should be calibrated to factor piracy as an additional ML risk.

Acquisitive Crime Generally

Any crime motivated by the prospect of making money can be the source of money laundering: human smuggling and tax evasion are but two examples.[43] A British report once declared that 70% of all crime was acquisitive.[44] The claim is not particularly backed by supporting evidence, but even if the percentage is suspect, the concept is familiar. There are crimes that lack an acquisitive motive, crimes of violence or impaired driving offences. In the main, most crimes, whether they involve the smuggling of

39 Kraska, J *Freakanomics of Maritime Piracy* (2010), 16 Brown J World Affairs 109at 113 to 115.
40 Bahadur, J *Pirates of Somalia* (Toronto: HarperCollins, 2011) p. 227.
41 UNODC *Awash with Money* (Vienna: UNODC, May 25, 2011) p. 1 reported $110 million; a subsequent FATF report suggested the range of $180-238 million FATF *Organized Maritime Piracy and Related Kidnapping for Ransom* (Paris: FATF, July 2011) at p. 8.
42 UN Security Council resolution 1950 in 2010 calls upon states to take part in the fight against robbery and piracy off the coast of Somalia.
43 See for example Simser, J *Tax Evasion and Avoidance Typologies* (2008), 11 J Money Laundering Control 123.
44 Cabinet Office (Performance and Innovation Unit) *Recovering the Proceeds of Crime* (London: Cabinet Office, 2000) at p.4.

contraband or the extortion of a local business, have an economic motive for the criminal. The more sophisticated the criminal, the more likely the crime will include money laundering.

Organized Crime

Organized crime creates an interesting dimension when considering AML risk. The criminal activities that a continuing criminal enterprise engages in can vary. If an organization has a pipeline to move drugs from source to market, that same pipeline can be used to smuggle humans, illegal cigarettes, guns, bulk cash or anything else that brings a profit. Diversification is a sound business strategy. One commentator has noted that globalization and economic integration across borders has created two interesting vectors: integration of economies makes cross-border crime and ML easier; to the extent that countries integrate to confront crime, organized crime finds cutting edge ways of cooperating with each other.[45] Organized criminal organizations tend to create a hierarchy: the operating minds, the bosses, do not get their hands dirty, a task delegated to associates, the expendable foot soldiers. The operating mind does, however, want the filthy lucre. Properly laundered money is the ideal method for organized crime; the wealth is distanced from the crime and conferred with the patina of legitimacy.[46]

Money Laundering Techniques. The early focus in our AML systems was on the traditional intermediary, the financial institution (typically a bank). The world has evolved rapidly since then. There is a constant stream of new actors, innovative technologies and novel mechanisms to transfer wealth. In Canada, AML rules are not limited to traditional gatekeepers in the financial system and apply to, amongst others, money service businesses, dealers in precious metals and stones, real estate brokers and developers.[47] The focus in a risk-based system is not merely on actors, ML activities are changing too. Policy makers must balance between the risk that our current AML system will fail to keep pace with innovation and the risk of an AML rule inhibiting innovation (a tension that plays out in prepaid access cards, discussed below). This section of the paper considers a number of traditional and emerging ML techniques

Placement or Loading Cash

---

45 Zagaris, B *International Enforcement Law Trends for 2010 and Beyond: Can the Cops Keep Up with the Criminals?* (2011), 34 Suffolk Transnat'l Law Rev 1 at 3.
46 See for example, Shikata, K *Yakuza organized crime in Japan* (2006), 9 J Money Laundering Control 416.
47 Although not lawyers, see *Federation of Law Societies of Canada v. Canada (Attorney General)*, 2011 BCSC 1270 (CanLII).

ML, at its most rudimentary stage, could consist of simply burying money in one's backyard or depositing money in one's account, hoping that it won't be identified. These steps aren't particularly effective. Buried money is at risk of irreparable damage or theft and isn't readily accessible.[48] Money deposited in a launderer's account is at risk of detection by law enforcement. The act of depositing money is at risk of being identified by the AML barriers to cash loading. Deposits over $10,000 trigger a currency transaction reporting or CTR obligation; unusual deposits can trigger a suspicious transaction reporting obligation (STR in Canada; suspicious activity report or SAR in the US).[49] Techniques to evade the AML regime have been developed, the most colourful names of which is "smurfing" whereby a series of cash deposits below the $10,000 threshold are made to evade CTR reports.[50] Cash is a point of vulnerability, particularly for drug traffickers. While the metrics are somewhat dated consider the following: 44 pounds of cocaine can produce $1 million, which when denominated in $10 notes, weighs 220 pounds (and takes up a lot of space).[51] The drug dealer will resort to a number of techniques. They may try and exchange smaller denomination notes for larger ones, a process sometimes referred to as refining; when bulk is a factor, a $100 note is preferred to five $20 notes. Curiously, in 2010 the American Treasury produced more $100 notes than $1 notes for the first time in history; of the 7 billion $100 notes in circulation, over two thirds of them are outside of the United States.[52] International drug cartels can also resort to bulk cash smuggling, that is moving money through to consolidation points and ferreting it across the border to countries will less rigid AML systems.[53]

Nominee Ownership

Another rudimentary method of "laundering" involves putting assets into the name of someone else. While basic, this method is not necessarily simple for a number of reasons. First, AML regimes have KYC (know your customer), CDD (customer due diligence) and EDD (enhanced due diligence) rules in place precisely to expose money

48 The Escobar cartel wrote off 10% of the cash holdings every year "because the rats would eat it or it would be damaged beyond use by water and dampness." Escobar, R (with D Fisher) *The Accountant's Story* (New York: Grand Central Publishing, 2009) p. 58.

49 STR is the Canadian term; in American parlance, SAR or suspicious activity report is used. For Canada see: *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17.

50 Welling, S *Smurfs, Money Laundering and the Federal Criminal Law* (1989), 41 Fla L Rev 287. For a case example see *R. v. Black*, 2009 NBPC 27 (CanLII).

51 Pricing cocaine is difficult. The price is not simply a product of quantity, but also of quantity, more specifically purity. Typically cocaine is diluted, or cut, by agents as it moves through the supply chain. Simser, J *The Significance of Money Laundering: the Example of the Philippines* (2006), 9 J Money Laundering Control 293 at 294.

52 Appelbaum, B *As Plastic Tops Cash* (New York: New York Times, p. 8, July 17, 2011).

53 Simser, J *Plata o Plomo: Penetration, the Purchase of Power and Mexican Drug Cartels* (2011), 14 J Money Laundering Control 266 at 273.

laundering through nominees. Second, the person has to trust the assignee. Criminals can be the victim of other predatory criminals, but cannot take the steps an honest citizen would (call the police or threaten a civil lawsuit) when their loot is stolen. As an alternative to a nominee relationship, a launderer can lay off the risk to intermediaries. For example, victims of a telemarketing fraud sent cheques to a fraudster; the fraudster in turn sold the cheques at a discounted rate to a Montréal restaurant owner, who in turn sold them on to a broker, who in turn sold them to a money exchanger in Jerusalem. Following a series of further exchanges, the cheques ended up with a money exchange business in Ramallah, who presented them to U.S. financial institutions to be honoured. While law enforcement eventually unravelled the case, it was a difficult task; further there was an immense of time and space placed between the fraudster (who got his money in Montréal) and the Ramallah money exchange.[54]

Sometimes nominee owners are easily dispatched. In an Ontario forfeiture case, cash was seized from a young man. His father claimed the cash in court (although not the marihuana and scales it was found next to); the father claimed that the cash was the residue of an "educational fund" that he had created for his son. Following a review of the son's extensive criminal history, the court rejected the father's claim:

I acknowledge that "hope springeth eternal" but would conclude that any reasonable person have regard to the course that Adam's [the son's] life has followed would agree that there is no likelihood that Adam would be pursuing higher education and be in need of the $9,780 to fund his education.[55]

Trusts and Corporate Entities

A legal trust is another nominee technique. A trust is a legal relationship: property is held by one person, generally called a trustee, for the benefit of another, generally called a beneficiary. A third person, sometimes called the settlor, can fund the trust. So for example, I could set aside money for my daughter through my personal lawyer: the lawyer is the trustee (and to the outside world may appear to be the "owner") while the daughter is the beneficiary and I am the settlor. This kind of arrangement is perfectly legitimate; however, it is not hard to see how a launderer could abuse this form of transaction. CDD requires a financial intermediary to know who the beneficial owner is in any relationship. For a number of reasons, offshore trusts can create the opacity that a launderer desires. Some jurisdictions offer additional barriers in their trust laws:

---

54 Simser,J *Money Laundering and Asset Cloaking Techniques* (2008), 11 J. Money Laundering Control 15 at 17.
55 O*ntario (Attorney General) v. Bixby*, [2004] OJ 6214 (SCJ) at para 14.

narrow definitions of fraudulent transfer, short limitation periods, elevated standards of proof to open up a trust and a refusal to recognize orders from other countries. Trusts themselves can be settled with a "flight" clause: the governing law or location of the assets can be changed upon a triggering event, such as service of an injunction or a warrant. Instead of a trust, privately held corporations can operate as a simple method for holding assets. As a rule it is difficult to determine who the shareholder is and generally there's lax supervision over the filing requirements for officers and directors. Corporations are, legally, persons; assets of the corporation can be paid out to investors through shareholder dividends, to officers through salaries, to business partners through the purchase of goods/services or to lenders through loan repayments.[56] Again, CDD when properly applied requires an institution to identify who the shareholders are in a corporate structure.

Asset Stripping

Financial instruments and business entities can be structured to allow value to move between and amongst parties over a range of transactions. The overwhelming majority of these transactions are perfectly legal and form of the backbone of our modern economy. A clever launderer can manipulate transactions to strip and cleanse assets in a variety of ways. For example:

- **Corporate Transactions:** A chain of related corporate entities can move assets around, falsify transactions, hedge risk by encumbering assets, pay salaries of dividends or create other revenue streams for the launderer which appear, to at least the casual observer, to be legitimate. Playing across borders in various jurisdictions adds informational asymmetry to the picture. Money can flow out of the country to pay a fictitious invoice and then be integrated back when that company "lends" money to the launderer or pays off his credit card bills.[57]
- **Leases**: generally speaking, law enforcement agencies won't seize a fully leased piece of property, like a car; a lease is an obligation, not an asset. If I want to have a vehicle and insulate myself from the prospect of forfeiture, I'll likely lease it. If I want to launder my money into that vehicle, I may seek a lease that is highly loaded at the front end. For all intents and

56 Simser, J *Money Laundering and Asset Cloaking Techniques* (2008), 11 J. Money Laundering Control 15 at 17 to 19.
57 For example, Mr. Holliday had a series of Atlanta escort agencies; he created a company in Nevada and another on the Isle of Man. Holliday had the offshore entities bill his Atlanta escort agency for fictitious services; after the invoices were paid, Holliday borrowed the money under a promissory note and used a credit card paid off by the offshore entities: Simser,J *Tax Evasion and Avoidance Typologies* (2008), 11 J Money Laundering Control 123 at 126-127.

purposes, the fact of the lease makes the vehicle less susceptible to seizure. If law enforcement were diligent and checked beyond the fact of the lien, they might learn that ninety-nine percent of the lease is paid off, but this step doesn't always occur.

- **Joint Tenancies**: if I want to protect the interest of my life partner, I can structure ownership through any number of devices. In a tenancy in common, my partner will have an interest, however defined, in the property; in a joint tenancy, a similar ownership structure exists, except that if I die, my share in the property passes automatically (or through the legal instrument setting up the joint tenancy) to the other owner.[58]
- **Insurance**: a launderer can take out a life insurance policy based on substantial initial payments and then surrender the policy later for early redemption or cash it out during the "cooling off" period. While the transaction does not make economic sense, given the penalties in the policy, the insurance company cheque appears to be a clean source of funds.[59]

Exotics: Derivatives

Broadly speaking, derivatives are financial instruments, created through a contract, that define a relationship between an underlying asset and a quality that is "derivative" of that asset. The derivative quality can be one of an infinite number of things: interest rates, commodity prices, foreign exchange rates and so on. Conceptually derivatives allow parties to either hedge or speculate on risk; the amount of market activity for derivates is staggering.[60] A simple form of derivative is a futures contract; parties agree to buy or sell an asset at a future date for a particular price. Swaps allow parties to exchange cash flows from different asset pools at a future date. For example a mortgage company could swap some of their fixed income flow with the variable interest flow of a credit card issuer; both parties can hedge a number of risks (fluctuating interest rates, borrower default and so on). The vast majority of derivatives are used like this to hedge risk on matters like commodity prices or the cost of foreign currency. Some derivatives are used for speculation, which can bear enormous risks (UBS

58 Although a joint tenancy in and of itself still creates challenges, particularly for uninvolved interest holders. Consider *BJF v. The State of Western Australia*, [2011] WASC 163.

59 See for example FATF *FATF Money Laundering and Terrorist Financing Typologies* (Paris: FATF, 2005); See also the New Zealand case of *Reid and other v The Queen* [2007] NZSC 90 where an insurance policy was used as part of a fraudulent tax avoidance scheme.

60 By the end of 2010, the over-the-counter derivatives market reached $601 trillion: Bank of International Settlements *OTC Derivatives Market Activity in the Second Half of 2010* (Basel: BIS, May 2011).

reportedly lost $2.3 billion in 2011).[61] Derivatives, like any financial instrument, bear the potential for money laundering. There would need to be a breach of a number of AML systems, either through subterfuge or the corruption of insiders, however, the amount of money that could be laundered is potentially massive.

Trade-Based Money Laundering

Trade-Based Money Laundering or TBML is a variation on the nominee owner technique and uses imports and exports to move value from party to another, facilitating ML. There are many techniques. The simplest can involve under-invoicing or over-invoicing the price of goods; the cash differential on the price is the vehicle to cleanse the money. For example, Escobar's notorious Columbian cartel used TBML with Columbian emeralds. A cartel associate in the US or Spain would place a multi-million dollar order for emeralds. The stones shipped against the order would be inferior and worth considerably less than the face value of the order. Inferior emeralds would be injected with oil; for a customs inspector, the shiny emeralds appear to have the attributes on the bill of lading.[62] The difference between actual value and the value on the bill of lading would be diverted as "cleansed" money. Escobar's accounts would show emerald trading, not cocaine shipments.

There are numerous TBML typologies, the most typical of which involve the intentional misstating of price, quantity or quality of goods shipped.[63] This technique takes advantage of more than 3,000 free trade zones (FTZs) in 135 countries. FTZ's are set up to encourage exports, providing: exemptions from duties and taxes; simplified administrative procedures; and, duty-free importation of raw materials. FTZs tend to have relaxed enforcement standards, something complicated by the practice of trans-shipping from smaller ports to larger regional ports.[64] AML systems can look for various "red flags" including: oddities in the underlying transaction (is method of payment inconsistent with standard practice for that type of risk? Are there unusual cash transactions?), unusual business activity (is the product transhipped for no apparent business reasons?) and discrepancies in the documentation (is the document consistent with business practices? Are there frequent amendments to letters of credit? Is the shipment outside the normal scope of that entity's business activities?). The use of intermediaries and nominees, like front or shell companies, poses an additional risk.

---

61 UBS recently suffered $2.3 billion in losses following speculations by a rogue trader in their organization: http://www.ft.com/indepth/ubs-rogue-trading-scandal (last viewed October 19, 2011).
62 Escobar, R (with D Fisher) The Accountant's Story (New York: Grand Central Publishing, 2009) at p.75.
63 McSkimming, S *Trade-Based Money Laundering: Responding to an Emerging Threat* (2010), 15 Deakin LR 37.
64 Liao, J; Acharya, A *Transshipment and trade-based money laundering* (2011), 14 J Money Laundering Control 79.

An additional flag should be raised if those entities are incorporated in tax havens.[65] That said, the AML system is not well placed to identify TBML; eighty percent of trading is done on an open account basis and intermediaries, like banks, see little if any documentation.[66] Banks don't, to stay with an earlier example, inspect emeralds.[67]

Artwork is also susceptible to TBML. Works of art are difficult to valuate, so as with emeralds, it is relatively easy to over or understate the value. Stolen artwork is traded in the underworld: exchanging drug money for a piece of art doesn't actually launder the money, but it leaves the trafficker with something priceless to enjoy (even if it's hidden away in a mansion). The art industry is shrouded in secrecy and largely unregulated. There are a myriad of money laundering techniques: a dealer may take cash (without the requisite CDD); there can be multiple invoices for the same artwork; and back-to-back loan schemes can be used to launder money through art.[68]

Diamonds are also susceptible to TBML. So-called blood diamonds have fuelled conflict in places like Angola, Sierra Leone and the Democratic Republic of the Congo. The Kimberly Process has created some controls, particularly a rough diamond certification process designed to ensure that the source of the stones were known.[69] That said, all diamonds, regardless of origin, are valuable and easily transported. In theory they can be traded anywhere in the world; a Toronto dealer that converts his drugs to diamonds can easily exchange the stones in Ankara or Moscow for U.S. dollars.

Pump and Dump: the Stock Market

A "pump and dump" scheme is a fraudulent manipulation of the capital markets. Often run out a "boiler room"[70] sham promoters will manipulate a company listed on a junior market. Investors, or rather victims, are pushed through aggressive sales techniques to buy the shares. Experienced fraudsters will know when the company's shares will peak, as the share price is related not to underlying values but the scam itself. This presents

---

65 FATF *Money Laundering Vulnerabilities of Free Trade Zones* (Paris: FATF, March 2010) at pp. 31 & 33.
66 Deltson, R; Walls, S *Reaching Beyond Banks: How to Target Trade-Based Money Laundering and Terrorist Financing Outside the Financial Sector* (2009), 41 Case W Res J Int'l L 85 at 106.
67 Simser, J *Money Laundering: Emerging Threats and Trends* (slated for publication in 2012 in the Journal of Money Laundering Control) at pp. 15-16.
68 Purkey, H *The Art of Money Laundering* (2010), 22 Fla J Int'l L 111.
69 Their website, www.Globalwitness.org contains a number of library items including: http://www.globalwitness.org/library/few-dollar-more-how-al-qaeda-moved-diamond-trade last viewed July 11, 2011. See also Harrington, A *Faceting the Future: The Need for and Proposal of the Adoption of a Kimberly Process-Styled Legitimacy Certification System for the Global Gemstone Market* (2009), 18 Transnat'l L & Contemp Problems 353.
70 The scamsters don't need the "legitimate" office space that a legitimate brokerage firm would and can run out any space that phones will work in, even the boiler room of a building. Scamsters can use phones and apparently emails as well to pump up a stock, see: *Hypo Alpe-Adria-Bank (Lichtenstein) AG (Re)*, 2007 BCSECCOM 622 (CanLII).

an interesting money laundering opportunity. Instead of paying for an illicit commodity with cash, a deal can be arranged whereby the seller takes shares prior to the scam; these might be worth a nominal amount. The seller can then dump their shares at the same time as the operating mind of the boiler room; the fraudster knows, through their own manipulation, when the acme of the market occurs. In this way, a fraudster could diversify, purchasing drugs in exchange for the proceeds of some of his scam. All an AML system would show are earnings from the stock market and the money would effectively be cleansed.[71]

New Payment Method Typologies

New payment methods (NPMs) are one of the fastest developing products in the financial services. One type of NPM, the prepaid access card, was created to facilitate online transactions and to assist the unbanked and underbanked. Four million American recipients of social security lack a bank account; they rely on prepaid access cards to receive a benefit.[72] NPM typology studies in 2006 and 2010 concluded that they are misused as a method of third party funding (using straw men and nominees) and to exploit both of the non-face-to-face nature of the transactions and NPM providers themselves.[73]

Prepaid access cards are an NPM device whereby value is paid in advance and extracted later. The cards can nest in closed network or loop (a gift card for a store or a Metro card for the transit system). Alternatively, open loop cards, like a prepaid Visa or MasterCard,[74] can be used for virtually anything. The prepaid access card allows a customer access to a shared pool of funds; the card itself holds no value, the system it accesses does. For example, if I present my card at the point of sale, the terminal I swipe into asks the system a question: is there sufficient value to support my proposed transaction? When the answer is "yes" the card's issuer (or a third party processor) tells the vendor "okay" and I complete my purchase. A notional hold is placed on the balance identified with the card and the transaction is later settled between merchant and issuer.[75] Prepaid access cards were created in Italy in the 1970s when pay phones

71 Simser,J *Money Laundering and Asset Cloaking Techniques* (2008), 11 J. Money Laundering Control 15 at 17 to 19 Simser,J *Money Laundering and Asset Cloaking Techniques* (2008), 11 J. Money Laundering Control 15 There was evidence in the appeal of a convicted money launderer that he'd also been involved in pump and dump schemes: *R. v. Rosenfeld*, 2009 ONCA 307 (CanLII).

72 Financial Action Task Force ("FATF") *Money Laundering Using New Payment Methods* (Paris: FATF, October 2010) p. 12.

73 Ibid, see also FATF *New Payment Method Report* (Paris: FATF, 2006).

74 These credit card companies issued prepaid cards in 2001: Albers, J *Stored Value Cards: Should we know the Holders?* (2007), 11 NC Banking Instit 363 at 369-71.

75 Linn, C *Regulating the Cross-Border Movement of Prepaid Cards* (2008), 11 J Money Laundering Control 146. See also: Dept. of Treasury *Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations & Definitions and other*

were regularly broken into to steal coins. Phone cards replaced those coins. Two decades later, long-haul trucking companies used prepaid cards as a payroll device; with drivers constantly on the road, mailing a paycheque was difficult. The prepaid access card could be loaded remotely by the trucking company and accessed by the trucker at a truck stop ATM anywhere.

The *Credit Card Accountability Responsibility and Disclosure (CARD) Act, 2009*.[76] brings prepaid access cards into the American AML regime through Department of Treasury regulations posted in July 2011.[77] Under those regulations, suspicious activity reporting and CDD is required for both sellers (retailers) and providers; providers also need to register with the American FIU, FinCEN (given the dispersal of the product, this might prove challenging but the regulations articulate a process for resolving the challenge). There are numerous exemptions (prepaid access products of $1,000 or less, payroll products provided conditions are met, closed loop cards of $2,000 or less and governmentally funded cards). The regulations focus on the actors, not the products. Treasury has proposed to accord prepaid access cards with the status of a monetary instrument, meaning, for example, that there will be a requirement for travellers to declare at the border prepaid access cards; cards, cash and possibly cell phones are to be aggregated and if they are valued at $10,000 or more, a reporting obligation on the traveller is created.[78] This may still entail challenges. There's no articulated method for law enforcement to "seize" money laundered into a prepaid access card.[79] Keep in mind, the money isn't actually "in" the card, the card is merely a conduit through which a system is accessed to transfer value.

In October 2011, America's FIU reported on common typologies related to suspicious international prepaid card activities.[80] A review of just under 800 SARs (STRs in other parlance) showed withdrawals at foreign ATMs, transactions with foreign websites and international wire transfers as the main suspicious activity (mostly reported by banks). The report confirms that fraud is a primary area of risk. These cards can be used, for example, in identity theft and fraudulent account takeover. The fraudster then typically

---

Regulations relating to Prepaid Access (Washington: Dept of Treasury document 4810-02, June 2010). In Canada, the larger issue of payments systems is being studied, see: http://paymentsystemreview.ca/ (last viewed August 8, 2011).

76 Public Law 111-24.

77 Department of the Treasury (Financial Crimes Enforcement Network) *Bank Secrecy Act Regulations & Definitions and Other Regulations Relating to Prepaid Access* (July 29, 2011), 76:146 Federal Register 45403 & 45420.

78 FinCEN Proposes Reporting Requirement, October 12, 2011 see: http://www.fincen.gov/news_room/nr/pdf/20111012.pdf (last viewed October 31, 2011).

79 Leino, R *The Strange Case of Amended Amendment S.A. 1107* (2010), 13 U Pa J Bus L 301 at 315 & 317 See Linn, C, *Op Cit* Note 25 particularly at p. 157.

80 FinCEN *SAR Activity Review: Trends, Tips and Issues* (Volume 20) (Washington: FinCEN, October 2011) at p. 13.

uses the card with international cash withdrawal capabilities to move the money beyond the reach of either the victim or law enforcement.

E-Money

Commodity-backed electronic money (e-money or digital currency) is an evolving area that potentially poses an AML risk. A typical digital currency is backed by an asset like gold. The issuer holds bullion and then contracts through exchange agents who sell the digital currency to end-users with cash or a wire transfer. The end user can then use the electronic currency online. Transactions, unlike credit cards, are generally of a non-recourse nature; there's no charge back process to challenge a merchant and the currency provider will not make a dissatisfied consumer whole. The exchange agent can exchange electronic money for a fiat currency (dollars, euros and so on). Electronic currency is used for on-line role playing games (users may be too young to get a credit card) and for online gambling and pornography where users desire anonymity. Some systems, like GoldMoney operating out of New Jersey, have stringent verification systems; many others promote the anonymous nature of their services. The theoretical risk of money laundering is very real; the current reality is much less certain. The industry itself is developing and unstable. Not everyone trusts the issuers and exchange agents; electronic currency doesn't generally operate in the brick and mortar world, nor is it widely accepted. Further, the challenges posed by e-money aren't always well understood. One commentator has stated that the AML threat "posed by digital currencies is mostly hype."[81]

P2P Transactions

Internet-based platforms have developed allowing individuals to transact with other individuals, either as an act of charity or as a money making investment. In particular, person-to-person (P2P) lending is growing rapidly. The American for-profit platforms (Prosper Marketplace and LendingClub) have facilitated 63,000 unsecured loans worth $469 million by March of 2011; Zopa, a British lender, had £125 million in loans. The American not-for-profit Kiva Microfunds had over 273,000 interest-free loans, mostly to developing world entrepreneurs, worth $200 million. For-profit P2P loans average between $6,000 and $10,000 and are made primarily to consumers (often to pay off or consolidate debt). A lender can advance all of a loan or take a percentage of a loan in increments as small as $25. The lender purchases payment dependent notes from a

81 Tucker, P *The Digital Currency Doppelganger* (2009), 17 Cardozo J. Int'l & Comp L 589. See also Merlonghi, G *Fighting Financial Crime in the Age of Electronic Money* (2010), 13 J Money Laundering Control 202.

P2P company; the individual lender bears the risk of non-repayment. The P2P company posts loan requests, interest rates and assigned letter grades (indicating credit risk). The P2P company then works with a chartered bank (e.g. WebBank of Utah) who disburses the loan and assigns it back to the P2P. Money is collected by electronic funds transfer and the lender is repaid, less a service fee of 1%. The top three grades of loans have less than a 1% default rate. The not-for-profit sector operates differently. Kiva, for example, collects from lenders and then distributes the money to 130 different micro lending institutions around the world. Those institutions, not Kiva, identify prospective borrowers, risk and are responsible for collections. The initial lender bears the risk of non-repayment but the loans do not earn interest for the lender. Loans do bear interest, however, for the borrowers who pay up to 37% to the micro lending institutions. Entrepreneurs in 59 countries have borrowed money through this vehicle. In the United States the regulatory response to this burgeoning industry is still being thought out. Currently *Bank Secrecy Act* rules, requiring CDD, SARs and so on apply to the WebBank and the P2P companies. Whether the unique circumstances of P2P lending work for the existing AML rules has yet to be determined.[82]

RDC

Remote deposit capture or RDC is an evolving financial services product that institutions offer primarily to business customers. A cheque can be deposited into an account from a remote location (an office for example) without having to physically deliver the cheque to the bank. American banks will accept a scanned image of the cheque, a service useful for customers wanting to go beyond the traditional deposit collection system.[83] A recent report by FinCEN, the American FIU, noted that RDC has posed problems from an AML perspective.[84] Some institutions have been penalized for inadequate AML controls. FinCEN noted that there is particular AML risk when transacting with international casa de cambio (CDCs) and money-service business (MSBs), a risk that extends to traveller's cheques. CDCs from Mexico and MSBs from a number of countries use RDC services to deposit cheques to correspondent accounts in the US. RDC has posed a number of risks including: double presentment of cheques (a cheque will be entered electronically and then be presented physically at a bank branch), counterfeit and altered cheques and cheque kiting. This is another example of a new financial services product presenting potentially unanticipated AML risks.

---

82 Government Accountability Office *Person-to-Person Lending* (Washington: GAO-11-613, July 2011); See also: Magee,J *Peer-toPeer Lending in the United States* (2011), 15 NC Banking Instit 139.
83 The Check Clearing for the 21st Century Act, Pub Law 109-100 authorized RDC in 2004.
84 FinCEN *SAR Activity Review: Trends, Tips and Issues* (Volume 20) (Washington: FinCEN, October 2011) at pp. 14 & 21.

On-Line Gaming

In April 2011, indictments were unsealed in New York against the three largest internet poker sites doing business in the United States (PokerStars, Full Tilt Poker and Absolute Poker). At the time of writing, the case is still before the courts, but the Department of Justice (DoJ) allegations, if proven, offer an interesting insight into the AML process.[85] In 2006, the U.S. government, concerned about on-line gaming, passed a law making it a crime to accept payment for internet gambling.[86] As part of their AML systems, financial institutions stopped processing payments. In the 2011 case, DoJ alleged that on-line gaming companies disguised gambling transactions as payments to hundreds of online merchants purporting to sell everything from golf balls to jewellery. Roughly one third of the transactions processed were alleged to consist of the gambling company's "rake" (a transaction fee for hands played). Another company allegedly set up phoney corporations and websites, which they parlayed into bank accounts; purportedly, financial institutions were not told that they were processing gambling payments. According to DoJ, financial institutions appear to have shut down accounts in 2009. The on-line gaming entities allegedly took a new tack, persuading a few small and troubled financial institutions to process payments in exchange for multi-million dollar investments. Prosecutors claim that the SunFirst Bank in Utah took a $10 million investment (giving up 30% of their equity) in exchange for processing payments.[87] If proven, this case shows that the AML system can create an effective barrier for the legitimate financial system.

Generally speaking, gaming has always posed ML risk. A launderer can take a spin around a brick and mortar casino, place a few bets and then cash out; as a result casinos file currency and suspicious transaction reports to FIUs all over the world. The same is true of online gaming. In order to access a poker site, a prospective gambler downloads their software, creates a profile and then funds an e-wallet. Gaming entities can then issue winnings through the e-wallet system in a cheque form. The system, from an AML perspective, is only as strong as the e-wallet provider: if dirty money can be funnelled into the e-wallet, unbeknownst to the gaming entity, a "clean" offshore cheque can become the source of laundered funds. One commentator has suggested

85 The case will take, minimally months if not years to resolve. See for example: http://www.justice.gov/usao/nys/pokerstars.html last viewed November 1, 2011.
86 *Unlawful Internet Gambling Enforcement Act*, found in Title VIII of the *Security and Accountability for Every Port Act 2006* (Public Law 109-347).
87 U.S. Attorney for the Southern District of New York *Manhattan U.S. Attorney Charges Principals of Three Largest Internet Poker Companies* (New York: Dept of Justice, April 15, 2011).

that law enforcement actions drove reputable e-wallet providers out of the American market, raising the risks of money laundering.[88]

Professional Sports Clubs

Recently, the Financial Action Task Force (FATF) examined money laundering typologies in sport, concentrating on the beautiful game of football (soccer to American readers). The FIFA World Cup in 2006 attracted 1 billion viewers, 15 percent of the world's population.[89] FATF warns that financial transactions which merit attention from an AML perspective include: opaque ownership structures, the European transfer market and ownership of players, betting activity and sponsorship. In a case from France, a money losing amateur club balanced their budget each year through financial infusions from the corporate holdings of a local businessman (he was illegally misusing corporate assets).[90] A Mexican case involved a local man of humble origin who, after five years away, returned to his home town and purchased a local football club. In fact he moved the club from an urban location to his small town of 30,000 people (the smaller market being a counterintuitive business transaction). His new club proudly outspent rival teams for players, coaches and infrastructure. They were promoted to the next division. The owner was later identified as a leader of a drug trafficking network.[91]

FATF have identified a number of AML risks associated with football clubs including:

- Football is a cash business (at the gate, in merchandise and in the concession booth) with the need for large influxes of capital. That capital can be sourced from a variety of stakeholders, supporters and sponsors. Observers of the player transfer market know that money is not always spent rationally;
- The culture of football is important: owners acquire a social status; young players may come from socially vulnerable environments; the allure of the sport can give owners access to and influence over politically exposed persons.[92]

---

88 Alexander, G *The US on Tilt* (2008) Duke L & Tech 6; see also Crutchfield, R *Folding a Losing Hand* (2009-10) 45 Tulsa L Rev 161.
89 FATF Money Laundering through the Football Sector (Paris: FATF, July 2009) at p. 9.
90 Ibid p.17.
91 Ibid p. 18.
92 Ibid p. 36.

Anti-Money Laundering or AML Systems. Anti-money laundering or AML systems are designed with two primary goals. One, AML systems impose barriers designed to impede the entry of dirty money into the financial system. Two, AML systems help law enforcement follow the money trail to identify culprits and seize their illicit money. AML systems were initially developed in the United States in the 1970's to combat offshore tax evasion, but they became important weapons to address drug trafficking.[93] In 1989 the International Monetary Fund and World Bank established a new group, the Financial Action Task Force (FATF) to encourage the adaptation of AML systems. In 1995 a network of Financial Intelligence Units (FIUs) was formed at a meeting in the Egmont-Arenberg palace in Brussels; the Egmont group was formed (they have over 120 members now).[94] Starting in 1999, countries that refused to implement AML systems were placed by FATF on a black list of non-cooperative countries and territories (NCCT). Countries went to great lengths to avoid the potential international isolation; tiny Nauru abolished 400 shell banks and implemented an AML regime to terminate their NCCT listing; the Philippines passed AML laws, fearing that the country might be cut off from the international financial system.[95]

The Foundation of AML Systems

In a 2006 article, Michael Levi and Peter Reuter posited that there were two pillars to the AML system: prevention and enforcement.[96] Prevention measures are designed to deter dirty money from entering the system and to provide for transparency, through reporting, to discourage institutions from participating in money laundering. Enforcement measures are designed to investigate and punish those who manage to evade the AML barriers and launder their money. Prevention measures have four key elements: customer due diligence (CDD), reporting, regulation/supervision and sanctions. AML prevention relies on gatekeepers in the system, particularly financial institutions, to assess and disclose risks to the authorities, often through the financial investigation unit, or FIU, in the appropriate jurisdiction.

Prevention

---

93 *The Bank Secrecy Act of 1970*, 31 U.S.C. §§5311 & 5314; the *Money Laundering Control Act of 1986* 18 U.S.C. §1956 and §1957 laid the basis for prosecutions.

94 See: www.egmontgroup.org one can also look to a number of other international bodies that play a role in AML systems ranging from the United Nations Office of Drugs and Crime on through to the Basel Committee on Banking Supervision.

95 Simser,J *The Significance of Money Laundering: the Example of the Philippines* (2006), 9 J Money Laundering Control 293 at 293-294.

96 Levi, M; Reuter,P *Money Laundering* (2006), 34 Crime & Just 289 at 297-98.

A risk-based approach, as opposed to a rigid rules-based system, has become the foundation for most AML systems. The first step is for the institution to understand and verify who their client is, hence CDD. As discussed earlier, there are good prudential reasons as to why an institution needs to not only know who the legal owner is, but also who the beneficial owner of the enterprise is. Institutions are expected to ask questions. Is the client a legitimate operating business? Are there reasons to doubt the legitimacy of the client? Are there unusual transactions or intentionally opaque sources of finance? The second element of an AML system is reporting. Sometimes reporting is largely an automated matter: a cash deposit of $10,000 may require an institution to file a currency transaction report (CTR).[97] Suspicious transaction reports (STRs or SARs) are far more challenging: the institution must exercise judgment. For example, a series of related cash deposits of less than $10,000 might give rise to an STR if the institution believes that the depositor is evading the CTR process. Institutions like banks are heavily regulated; the functioning of an AML system is overseen by the supervision system. The final element of the prevention consists of sanctions: institutions that don't properly implement AML systems can be the subject of regulatory and even penal sanctions. For some institutions, reputational harm bears an even higher price.[98]

A fulsome discussion of best practices for an AML regime is well beyond the scope of this paper, but a few could be noted:

- The AML function should operate independently of a business line. In many of the marihuana grow operation cases I've worked on, money is laundered into a residence. For the unknowing mortgagee, this is a profitable loan, with high equity and consistent payments. Banks don't reward managers that turn down loans. Banks should reward managers that protect their institution through diligent application of the AML rules.
- In Canada, as in many countries, federally regulated financial institutions must employ a CAMLO or Chief Anti-Money Laundering Officer.[99] The CAMLO is responsible not only for regulatory compliance but also for the

---

97 In Canada, those reports go to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) pursuant to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000* c. 17 (see for example s. 12(1)).

98 Riggs Bank had developed a niche market, trading with other countries, particularly through their Washington embassies, but the institution's reputation was shattered by allegations that they'd laundered money implicated by corruption, particularly in respect of the Pinochet regime. The bank was eventually taken over and the name "Riggs Bank" disappeared from the marketplace. See Permanent Subcommittee on Investigations *Enforcement and Effectiveness of the PATRIOT Act; Case Study Involving Riggs Bank* (Washington: Committee on Governmental Affairs, 108th Congress Money Laundering and Foreign Corruption, 2004).

99 Office of the Superintendent of Financial Institutions *Deterring and Detecting Money Laundering and Terrorist Financing* (OSFI: December 2008, Guideline B-8) Canada http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/b8_e.pdf.

broader prudential risk management. Institutions are expected to ensure that corporate governance, including that of executives and the board is appropriated attuned to AML issues.

- Most AML people I've spoken to stress the importance of a "message from the top" approach to AML work, demonstrating to all members of the firm that this is an important issue, not simply a regulatory burden to be endured and where possible gamed.
- The risk based approach forces the institution to rely on their staff and their computer systems to identify possible ML transactions. Risks are reported over to the FIU (discussed below) through automatically generated reports (e.g. currency transaction reports for cash deposits of $10,000 or more) and through suspicious transaction reports (STRs). STRs are generated either through technology that monitors transaction patterns or through staff who note something unusual. Risk adverse institutions, fearful of regulatory or even prosecutorial sanctions, may get into the habit of protectively filing STRs on garden-variety transactions, just in case. The problem with this, as one commentator has pointed out, is that the AML system cannot work as it's meant to; there's too much white noise flowing in the system.[100]
- KYC or know your customer is a critical building block for any AML system. The art of money laundering often involves taking an inefficient pathway to misdirect and secret money. A bank official who knows their legitimate profit-taking enterprises could well wonder why transactions are structured in odd or unusual ways.
- As noted, firms are expected to employ CDD and in appropriate cases, enhanced due diligence (EDD). Customers operating in high risk environments or clients with dubious or unknown sources of wealth should be the subject of EDD.

The FIU

AML work includes institutional reporting to a financial intelligence unit or FIU, which creates an informational gateway between the financial institution and law enforcement. Again a fulsome discussion of FIUs is well beyond the scope of this paper. Using Canada as an example, here are a few key points about FIUs:

---

100 Demetis, D *Unfolding Dimensions of an Anti-Money Laundering/Counter-Terrorist Financing Complex System* (October, 2011: LexisNexis Emerging Issues Analysis 6019) at p. 12.

- Canada's FIU is the Financial Transactions and Reports Analysis Centre of Canada, better known as FINTRAC;
- Created in 2000[101] FINTRAC collects information on suspect financial activities from regulated institutions (through STRs, CTRs and voluntary disclosure reports);
- FINTRAC ensures that institutions comply with their AML obligations (record keeping, reporting and so on);
- FINTRAC does take on a public education role, which includes preparing reports on typologies;[102]
- FINTRAC holds that information and controls it in accordance with privacy laws. The FIU conducts analysis on the information; and,
- If the FIU determines, based on their analysis, that the information should be shared, the agency will then pass a report on to law enforcement, the tax authorities or the Canadian Security Intelligence Service (CSIS).

There are a number of evolving issues for FIUs:

- Information sharing across borders is generally done through bilateral agreements, although there are several multi-lateral bodies and frameworks. Any high level money launderer will use borders and different jurisdictions to misdirect or hide the trail; and,
- While there has been much work done on standardization across jurisdictions, particularly through bodies like the Egmont Group and the Financial Action Task Force, there's still work to be done.

Enforcement

The enforcement aspect of an AML system has four elements. First, the criminal law will identify money laundering offences, often in reference to a list of designated offences.[103] The next two elements, investigations and prosecutions, are needed to bring a matter to the courts. Finally, given that money laundering is really about hiding wealth, a variety of civil and criminal forfeiture laws can be used to deprive criminals of

---

101 Created under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17.
102 The reports can be found at: http://www.fintrac.gc.ca/publications/typologies/1-eng.asp (last viewed October 27, 2011).
103 The offence of money laundering is set out in s. 462.31 of the *Criminal Code*, R.S.C. 1985, Chapt C-46; s. 462.3 defines proceeds of crime in relation to designated offences, which generally consist of offences prosecuted by way of indictment (although there are carve outs).

the fruits of their unlawful activity. Enforcement is a very complex area, very much beyond the scope of this paper.[104]

Conclusions. There are immense flows of tainted money moving around the world at any given moment. Like a floodwater, this money is programmed to relentlessly seek out gaps in our AML system. Where money does flow past our gatekeepers, enforcement mechanisms have been erected for law enforcement to repair the damage. This paper has surveyed a number of predicate crimes, the headwaters if you will of ML activity. This paper has also looked at a number of techniques designed to create and exploit AML gaps. The one constant in this field is change. Money launderers are highly incented to game the system. Money launderers can prosper by adapting to change. In response, AML systems need to be flexible and rigorous to stem the tide.

For more information on money laundering, see Money Laundering, Asset Forfeiture and Compliance

Click here for more Emerging Issues Analyses related to this Area of Law.

About the Author. Jeff Simser holds law degrees from Queen's University at Kingston and Osgoode Hall Law School. He is an asset forfeiture specialist and has worked with jurisdictions in North America, Europe, Africa and Asia. He's the author of numerous publications in the AML field and his most recent (co-authored) book *Civil Asset Forfeiture in Canada* is about to be published by Canada Law Book. A companion volume on *Criminal Asset Forfeiture in Canada* is currently in production. While this article represents his personal views, not those of his employer, Jeff is a legal director with the Ministry of the Attorney General in Ontario. Jeff can be reached at jeffsimser@yahoo.ca.

104 I've co-authored *Civil Asset Forfeiture in Canada* slated to be published by Canada Law Book in 2012 and am working on the companion volume covering criminal asset forfeiture, each is hundreds of pages long.