Speech presented by Adam Graycar, Director, Australian Institute of Criminology:

"Money laundering"

at the International Policy Dialogue, "Tackling Cross Border Crime", Challenges of International Development Cooperation, Bonn, Germany, December 16, 2002

Adam Graycar
Bonn
December 16, 2002

Background commentary to Money Laundering Presentation at International Policy Dialogue

This background commentary is designed to accompany the presentation.

Summary

The presentation surveys current efforts of developing anti money laundering at the government level and at the corporate level. In each case, the objectives are the same, but differences in orientation mean that there has to be an ongoing dialogue as to what is required at the national level and what is feasible at the corporate level.

Prior to September 11, 2001 the main thrust of money laundering was evasion of tax and conversion of illicit gains. Post September 11 (though evident leading up until then), an added dimension has been the laundering of money to finance terrorist activities.

As a consequence, the importance of partnership between government and the corporate world takes on a new essential focus - a movement in harmony, and concerted efforts in prevention, detection, enforcement and fundamentally in ***discerning patterns of activity*** that suggests criminal intent. This brings in new work on neural networks.

One broad repercussion of introducing best practice AML programs in financial institutions is that it will intrude on privacy issues. The question here is to what extent should such intrusions be tolerated in the interests of national security.

According to an Associated Press report (Catherine Wilson, AP Business Writer, Miami Beach, Florida, 21/2/02), nineteen of the twenty or so 9/11 terrorist hijackers had been identified pre-Sept. 11th, but they were a virtual blank to U.S. intelligence agencies. A British banking compliance company had, however, profiles of at least fifteen of them on its own compliance file of high-risk people. Banking officials had access to the information, but the profiles evidently were never seen by U.S. intelligence agencies.

Slides 1 & 2

The essential activity of 'laundering' money is to reduce the risk of seizure and forfeiture of money that has been illegally obtained. The goal of the activity for the launderer is to convert one liquid asset into another asset, usually in a less liquid form, so as to make identification of the source of the acquisition as difficult as possible.

This ‘less liquid’ morphing includes conversion into physical assets such as real estate, yachts, motor vehicles. These are obvious termination points, but the objective can also include monetary instruments such as financial securities or monetary transfer certificates, which may then be used as intermediary objectives towards achieving a more sophisticated and perhaps sinister objective, including terrorism.

However obtained, it should be recognized that money is only a means of exchange, a transactions medium, rather than an end it itself. So ‘hiding’ this dirty money does not constitute the crime of ‘money laundering,’ but rather merely points to evidence that it may have indeed been illegally obtained. Today - at the heart of most anti ML strategies - there is a focus on *discerning patterns of activity* that suggests criminal intent.

Slides 3, 4, 5
The stakes are high, not only because of *direction* the funds so obtained may take, but also because of the *magnitude* of the funds involved. By any system of reckoning, the total movement of funds worldwide has now reached a stage that defied comprehension only a few years ago.

In the most recent account, estimated by BNP Paribas on 25 October 2002, about $A1.56 *trillion* has been laundered around the world this year, with authorities only able to detect 0.1 percent of the total. By contrast, in 1998, the new US Financial Crimes Enforcement Network, or FinCEN, estimated that over $US750 *billion* in illicit funds was laundered globally; of which almost half was laundered through the United States.

Slide 6
The effect of money laundering causes ripples, like a stone being thrown into calm water: the justice and taxation systems are victims as well, as may well be the wider community and in the case of money laundering designed to fund terrorism, the wider world.

The four quadrants of this slide highlight the ripples for
- Offenders
- Victims
- Bystanders &
- the Justice system

Slides 7 – 12
The bombing of the twin towers in NYC on September 11 2001 was a watershed as far as money laundering was concerned.

This single act showed that the largely non-random redistribution of wealth towards criminal elements of society needed to be addressed, preferably head-on, but if not, obliquely, by the enactment of tougher anti ML laws. Some means of control were urgently needed to stem the flood of cash to unchecked hands. Put bluntly, the unstable movement of such large quantities of purchasing power in the wrong hands could threaten the very basis of civilised society. Once the ill-gotten gains are legitimately ‘placed’ into the financial system, the perpetrators of criminal activities can then invoke the law to protect their ownership of their coveted assets.

Slide 13: title only
Slides 14 – 20 incl
Financial institutions and corporations and other large organisations like government agencies are prone to ML activities. Modern technology enables people to fraudulently obtain new identities – often those of existing people – and from this base, obtain other documentation. Related to this is the ability to have mail redirected for nefarious purposes. From such simple beginnings it is only a short step to relatively sophisticated criminal activity. An example here is employees being able to have bank accounts opened in the name of their employer into which they then deposit and withdraw various monies / funds.

The Bank of International Settlements identifies the greatest risk as being a failure in various aspects of an entity's operations: processes, systems, people and external influences / events. The responsibility for addressing this lies with senior management, who should ensure that the right systems are in place for ensuring effective anti money laundering practices and that these systems, in fact, are working. Fundamental to this is the fact that all staff should understand their role and responsibility as regards minimising operational risk exposure.

The level of risk will differ from one entity to another and one industry to another; within an entity, the apportionment of operational risk will differ between products, activities, processes and systems.

Before any new process, system, activity or product is introduced, they should be assessed as to the level of risk to which they expose the entity.

One way of doing this is to assign appropriate values and plot the issue under question on a matrix, relative to the entity's other experiences / activities.

Slides 21 – 23 inc
In rolling out the *2002 National Money Laundering Strategy* in July 2002, US Treasury Under Secretary Jimmy Gurulé said that anti-money laundering enforcement has now become a priority in the Department. By attacking the financial structures of criminal organizations, you rob these organizations of their lifeblood. Called the Al Capone principle, because if you get Al Capone's money, you get Al Capone. It is one of the best ways to dismantle sophisticated criminal enterprises, he said. If you penetrate the financial underpinnings of a criminal organization, replacement is not so easy. The criminals can't just pick up the phone, Gurule continued, and find another sophisticated accountant or professional money handler who understands global banking systems, and is willing risk their comfortable white-collar lifestyle to venture into illegal waters.

The USA Patriot Act was in large measure, designed to address this. Signed into US law in late last year, the Patriot Act followed U.N. Security Council Resolution efforts to combat terrorism under many jurisdictions simultaneously, including the freezing of funds held by suspected terrorists. It provides an extensive battery of new powers designed to combat money laundering, especially if it has the potential to be used as a weapon of terrorism. Besides banks and Non Banking Financial Instituions, the provisions of this section will affect nearly other every type of financial service institution operating in the United States, including broker-dealers, registered and unregistered investment companies, money service bureaus, and life insurers.

The international implications of this are that if a bank in the Philippines for instance, wants to do business in the USA, it has to comply with new US banking laws. On a much larger scale, the imperative to comply is heightened in the advent of say, another 'Asian meltdown', when access to American dollars is critical.

Slides 24, 25
Complying with government requirements (like the Patriot Act in the US) means that banks now need to know a lot more about their client base than ever before. But the same now applies to the corporate sector, who now have to know their financial intermediaries and the business that they are in.

Slides 26, 27, 28
The complexity of new anti-money laundering initiatives requires careful consideration before application. Firstly, the ramifications of the paradigm shift are significant for a number of reasons, not the least of which is that they now allow for intrusive investigatory techniques to be applied as a preventive tool. Secondly, there is no doubt assistance of some sort or another will be required, both from law enforcers and financial institutions desiring to implement counter ML best practice/risk minimisation strategies. Acquiring specialist staff and setting up appropriate internal systems are steps in the right direction, but for serious applications computational assistance may be necessary.

In Australia, *Best Practice* is typified by AUSTRAC, a Federal Government agency that monitors banking transactions through Structured Query Language techniques that examine databases.

Another approach is to use Artificial Neural Networks. Derived from state-of-the-art military technology – as used for instance on Aegis-class destroyers for identifying and monitoring enemy activity across a broad spectrum – Artificial Neural Networks see connections between events that reveal far more than the events themselves. ANNs draw out relationships between seemingly unconnected pieces of information.

Last Slide: conclusion