Practice Note

Anti-Money Laundering Legislations and CFO Responsibilities

Janek Ratnatunga[1]

The business news that has dominated Australia in early August 2017 was the crisis that hit the Commonwealth Bank of Australia (CBA); which involved allegations of 53,700 contraventions of money laundering and terror financing laws by the Bank. It was alleged that repeated warnings were sent to the bank by the Australian Federal Police and Austrac (an Australian Federal organisation set up to implement the Anti-Money Laundering and Counter-Terrorism Financing Act of 2006).

It is reported that many of these warnings were allegedly ignored. There were supposedly mass deposits by syndicates, many with fake names, others featuring zombie account owners — flushing hundreds of millions of dollars in cash through CBA smart ATMs, with money then going offshore and in and out of other accounts. The new term “cuckoo smurfing” was introduced into banking parlance.

Amidst all of these allegations, what caught my eye was a snippet in the Business Review section of the Weekend Australian (August 12-13 2017) as follows:

“When the door swung open to the Colonial Theatre at CBA’s head office in Sydney at 2pm on Thursday, a phalanx of photographers lit up Ian Narev (the CBA Chairman) and his new Chief Financial Officer Rob Jesudason like Christmas trees. Mr. Jesudason, who until recently was living in Hong Kong as a senior executive with CBA, was new to the experience (he had taken up his new role only on July 1 2017) and seemed a little unnerved by his split-second transformation from anonymous banker to hunted public figure.

As a large percentage of ICMA members are CFOs, many in leading international corporations, I thought it is best to inform our members of the dark world of money laundering; and in this age of digital disruption how a simple error in computer code can make their organisations, often inadvertently, into money laundries.

The CBA case also shows that even with intimate knowledge of the digital world, a CFO can get caught off-guard; as Mr Jesudason’s previous role (whilst based in Hong Kong) was to spearhead CBA's digital banking growth strategy for its South African mobile venture Take Your Money Everywhere (TYME).

Money laundering is the process of making illegally-gained proceeds ("dirty money") appear legal ("clean"). In a number of legal and regulatory systems, however, the term money laundering has been extended to other forms of financial and business crimes, and is sometimes used more generally to include the misuse of the financial system (involving things such as securities, digital currencies, credit cards, and traditional currency); including terrorism financing and evasion of international sanctions. Most anti-money laundering laws link money laundering (which is concerned with source of funds) with terrorism financing (which is concerned with destination of funds) when regulating the financial system.

[1] First Published: Ratnatunga, Janek, (2017),“Anti-Money Laundering Legislations and CFO Responsibilities”, *On Target,* ICMA Australia Newsletter, 21(4), July-August, pp.6-8

Typically, money laundering involves three steps: ‘placement’, ‘layering’, and ‘integration’.

First, the illegitimate funds are introduced into the legitimate financial system (placement). Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts (layering). Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean (integrated).

The ‘placement’ of dirty money can take several forms, although most methods can be categorized into one of a few types. These include "bank methods; smurfing (also known as structuring); using legitimate cash businesses (such as casinos); currency exchanges, and double-invoicing". Here are typical types of ‘placement’.

Structuring: Often known as smurfing, this is a method of placement whereby cash is broken into smaller deposits of money, used to defeat suspicion of money laundering and to avoid anti-money laundering reporting requirements. A sub-component of this is to use smaller amounts of cash to purchase bearer instruments, such as money orders, and then ultimately deposit those, again in small amounts. This is essentially what is being claimed in the allegations against the CBA.

Cash-intensive businesses: Here, a business that is typically expected to receive a large proportion of its revenue as cash (such as casinos, distilleries, parking garages, massage parlours and strip clubs) uses its accounts to deposit criminally derived cash. Such enterprises often operate openly to derive cash from its legitimate business, in addition to the dirty cash which the business will claim as received in its legitimate business operations. Service businesses are best suited to this method, as such businesses have little or no variable costs and/or a large ratio between revenue and variable costs, which makes it difficult to detect discrepancies between revenues and costs. For example, in the case of a casino, an individual can walk in and buys chips with illicit cash. The money is now ‘placed’. The individual will then play for a relatively short time using a few of the chips, cashing in the remaining chips, and taking the payment in a cheque (or at least get a receipt so they can claim the proceeds as gambling winnings).

Bulk cash smuggling: This involves physically smuggling cash to another jurisdiction and depositing it in a financial institution, such as an offshore bank, with greater bank secrecy or less rigorous money laundering enforcement.

The following methods of ‘placement’ are used when a corporate entity is used either knowingly or unknowingly:

Shell companies and trusts: Trusts and shell companies disguise the true owner of money. Trusts and other corporate vehicles, depending on the jurisdiction (such as in the State of Delaware, USA), need not disclose their true, beneficial owner. Such companies are sometimes referred to as ratholes.

Round-tripping: Here, money is deposited in a controlled foreign corporation offshore, preferably in a tax haven where minimal records are kept, and then shipped back as a foreign direct investment, exempt from taxation. A variant on this is to transfer money to a law firm or similar organization as funds on account of fees, then to cancel the retainer and, when the money is remitted, represent the sums received from the lawyers as a legacy under a will or proceeds of litigation.

Other methods of money laundering are as follows:

Buy Real Estate: Corporations or individuals purchases real estate with illegal proceeds and then sells the property. The proceeds from the sale look like legitimate income. Alternatively, the price of the property is manipulated: the seller agrees to a contract that underrepresents the value of the property, and receives criminal proceeds to make up the difference.

Assigning Life Insurance Policies: The assignment of insurance is the transfer by the holder of a life insurance policy (the assignor) of the benefits or proceeds of the policy to a lender (the assignee), for a particular reason such as a collateral for a loan. In the event of the death of the assignor, the assignee is paid first and the balance (if any) is paid to the policy's beneficiary. In the case of money laundering, a policy is assigned to unidentified third parties and for which no plausible reasons can be ascertained.

Trade-based laundering: This involves under or overvaluing invoices to disguise the movement of money.

Black salaries: A company may have unregistered employees without a written contract and pay them cash salaries. Dirty money might be used to pay them.

The ultimate method to set-up a money laundry is to Capture a Bank. Here, money launderers or criminals buy a controlling interest in a bank, preferably in a jurisdiction with weak money laundering controls, and then move money through the bank without scrutiny.

There are many examples from around the world where individuals have started the ‘placement’ of dirty cash via slot machines; moved on to buy the entire casino to make it easier to ‘place’ larger sums of dirty cash; then purchased other legitimate businesses to ‘layer’ the dirty money with the clean money; and ultimately ‘integrated’ the washed money by purchasing real estate and ultimately, getting a controlling stake in a bank.

Of course, one can hoard illicit cash and wait for a Tax Amnesty, that legalizes unreported assets in tax havens and cash, if they are declared within a certain period. Often such amnesties often charge zero or minimal tax on cash that is so declared. For example, the recent tax amnesty in Indonesia offered tax incentives and immunity from prosecution (although a small penalty needed to be paid). Here the Indonesian government tried to make it attractive for (former) tax evaders to declare their offshore funds to Indonesia's tax authorities and - if desired - repatriate these funds into Indonesia. India’s recent de-monetization debacle was an attempt to flush out the hoards of illicit cash; but without providing a tax amnesty, it was seen to be an abject failure.

In Australia, cash dealers (especially Banks) are required to report international funds transfer instructions (IFTIs) and significant cash transactions (SCTRs) to AUSTRAC electronically rather than on paper, where the cash dealer has the technical means to do so and their reporting volumes exceed 50 forms per year (all types aggregated). Suspect transaction reports (SUSTRs) may continue to be reported on paper, although this is not AUSTRAC's preference.

Against this backdrop, let us see if last week’s hyperbole and hysteria with regards to the CBA is justified. To do this one needs to consider what exactly CBA is being accused of despite headlines such as ““53,000-plus money laundering breaches”.

Yes, there were 53,506 ‘threshold transaction reporting’ (TTR) failures; i.e the mandatory reporting to Austrac of any single cash deposit of $10,000 or more.

Apparently, the only reason that CBA had so many of these TTR infringements is that back in 2011 it broke ranks with other big banks in Australia and allowed cash deposits of up to $20,000 in its so-called “intelligent” ATMs (IDMs) – other big banks limited such cash deposits (and still limits them) to $5000; and a coding error resulted in not reporting such to Austec.

Now the customers of other big banks can still make a $20,000 deposit “at one time” - they just have to break it down into (say) four $5,000 successive transactions so as not to be caught by the

mandatory TTR reporting to Austrac. However, those "four $5000 successive" deposits would, one assumes, be caught by the separate "suspicious matter report (SMR)" obligations of the banks.

Now it is common knowledge of most Australian business people that cash deposits of more than $10,000 are going to be reported (to someone); and any criminal or terrorist who is dealing in dirty cash will know this in even more detail - and not deposit cash above this limit. This is the reason for also having the SMRs: to pick up deliberate and structuring of cash deposits below $10,000.

In fact, as Austrac itself has noted, of the 53,506 TTR breaches, only 1,640 related to money-laundering parties, (amounting to $17.3 million); and only a further six might have been considered to be terrorism related. The SMR breaches amounted to 245; where the CBA allegedly failed to lodge a more specific SMR on time or failed to monitor customers.

Is the CEO and CFO responsible?

The TTR notification is an absolute obligation. Once CBA decided to allow cash deposits of more than $10,000 it had to make absolutely sure the automatic computer notification triggers worked.

Whilst it may have been initially a failure in computer coding; the CBA failed to actively monitor such transactions by conducting subsequent testing to see that the TTR triggers were working - and it failed to do that for a number of years. Even though it appears not to have been a conspiracy, it was an error that was completely unacceptable, both in law and in banking practice.

This is ultimately the CEO's and CFO's and CBA Board's responsibility.