

Combating trade-based money laundering risk – a call for a united front

Recent anti-money laundering (AML) guidance from the Wolfsberg Group on trade finance has again highlighted the need for a holistic approach to combating money laundering, terrorist financing and corruption. Emily Brayshaw explains why tackling trade-based money laundering (TBML) is a burden that Australian financial institutions cannot shoulder alone.



By Emily Brayshaw

IT IS WELL-KNOWN in AML circles that regulators and international bodies consider the field of trade finance to be a high-risk area for money laundering. The Financial Action Task Force on Money Laundering (FATF) released the *Best Practices Paper on Trade Based Money Laundering* in June 2008, which grew from case studies revealed in its paper, *Trade Based Money Laundering 2006*. Closer to home, AUSTRAC provided guidance on the topic in Case 12 – Tax Evaded Through Exporting Goods of the *AUSTRAC Typologies and Case Studies Report 2008*.

However, the Wolfsberg Group's¹ January 2009 paper, *The Wolfsberg Trade Finance Principles*, offers an interesting perspective on the issue. The paper confirms the Wolfsberg Group's commitment to the application of appropriate systems and controls in respect of trade finance products to mitigate money laundering and terrorist financing (ML/TF) risks and potential breaches of international and national sanctions, including the proliferation of weapons of mass destruction. The paper states, however, that the Wolfsberg Group does not 'believe that currently there is



¹ The Wolfsberg Group consists of the following leading international financial institutions: Banco Santander, Bank of Tokyo-Mitsubishi-UFI, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale and UBS.



sufficient evidence to support an assessment of this area as high risk for AML/Sanctions purposes'. It is not often that there is divergence of views on key matters such as what are high-risk services for money laundering between an influential body such as the Wolfsberg Group and the FATF and AML/CTF regulators.

So what can financial institutions do about it?

The Wolfsberg paper claims that around 80 percent of the world's finance is conducted under open account terms. This means that the buyer and seller agree the terms of the contract, the goods are then delivered to the buyer, and the buyer uses the banking system to pay the seller. The problem for the financial institution in identifying risks, the Wolfsberg paper states, is that it will see only the payment and will have no visibility of the transaction.

In practical terms, this means that beyond conducting standard anti-money laundering and counter-terrorism financing (AML/CTF) checks and sanctions screening on the clean payment, there is little that the financial

business can do. This can help the financial institution determine whether additional AML/CTF measures are necessary.

The Wolfsberg Group limited the term 'trade finance' within the context of its paper to two standard products used to finance international import and export: documentary letters of credit (LCs) and documentary bills for collection (BCs) because of the lack of visibility of transactions conducted under open account terms. These two products have trade-related records, such as invoices and travel documents that are sent through financial institutions. These records are examined by financial institutions for consistency with the agreed terms of the transaction, but access to these records also means that the financial institution has some information it can use to help identify and mitigate ML/TF risk.

AML/CTF systems and controls around trade finance

The Wolfsberg paper provides detailed, practical guidance on the types of controls that may be applied to LCs and BCs. As there is usually more than one financial institution involved in a trade finance transaction (i.e. the seller is a customer of Bank A, the buyer is a customer of Bank B), the guidance also sets

- The review of information about the relevant parties and transactions, including reviewing specific information before a transaction is processed;
- The screening of parties and jurisdictions against sanctions lists and other lists of high risk or prohibited persons; and
- The monitoring of any transactional activity completed or in progress to detect any matter that may be unusual or potentially suspicious. This may be easier said than done, as the members of the Wolfsberg Group believe that it is 'impossible to introduce any standard patterning techniques in relation to account/ transactional monitoring processes or systems' in trade financing.² This is because of the range of variations which are present even in normal trading patterns, the paper notes.

The paper also provides lists of risk indicators (or red flags) around LCs and BCs that financial institutions should consider pre and post-event, as well as a useful summary of key controls described in the guidance for these trade finance products. In addition, the paper discusses sanctions issues, including the need for customer due diligence, name screening and activity-based financial sanctions. With regards to the latter, the paper notes that financial institutions should be aware of United Nations resolutions in relation to the proliferation of nuclear weapons, weapons of mass destruction (WMD), dual use of goods and relevant local legislation which translates these into national laws or regulations.

The paper highlights the limitations and challenges in attacking TBML because financial institutions are only one of the relevant stakeholders in these transactions. It acknowledges that financial institutions are the 'primary conduit for the movement of funds' but states that 'substantial participation from other key stakeholders is required in order to provide an effective deterrence effort and to aid the detection/discovery of the relevant targets in this area'.³

The Wolfsberg paper calls for ongoing cooperation among government stakeholders, law enforcement, financial intelligence agencies, regulators, export credit agencies, customs and excise, tax authorities, shipping agents, carriers, port authorities and global bodies in identifying and mitigating ML/TF risk and preventing sanctions breaches. This echoes the call of FATF's 2008 paper on TBML to involve all of these parties in combating ML/TF – not just the financial institutions – and for them to receive training



institution can do to identify the presence of ML/TF risk indicators or detect unusual or suspicious activity. In some instances, such as when the financial institution is providing credit in relation to the transaction, there may be more opportunity to understand the underlying trade and financial movements, i.e. an opportunity to know the client's

out practical measures for Bank A and Bank B within four categories, tailored to meet their roles in the transaction:

- The conduct of due diligence on customers and related parties to the transactions, including enhanced due diligence when necessary;



² Page 8 Wolfsberg Trade Finance Principles January 2009

³ Page 31 supra.

on typologies and techniques, in conjunction with their global counterparts.

Inter-agency efforts on the home front

Some work is already taking place in Australia beyond the finance sector in terms of identifying and addressing ML/TF risk. For example, a number of government agencies deal with trade, sanctions and corruption issues as part of their remit. This includes AUSTRAC, the newly-renamed Australian Customs and Border Protection Service (ACBPS), state police forces, the Australian Federal Police, state revenue agencies, the Department of Foreign Affairs and Trade (DFAT), the Export Finance and Insurance Corporation (EFIC), the Attorney-General's Department (AGD) and the Australian Taxation Office (ATO). Many of these agencies have increased their AML/CTF focus in recent years through: training; establishing and boosting financial crime control teams; investigations; releasing guidance; and establishing hotlines to report suspected criminal activity including drug trafficking, bribery and tax evasion.

One of the government's recent anti-bribery measures has been to pass the *International Trade Integrity Act (ITIA) 2007*. The ITIA is a direct result of the Cole Inquiry Report into the kickback scandal



that dogged AWB and amends existing legislation to, among other things:

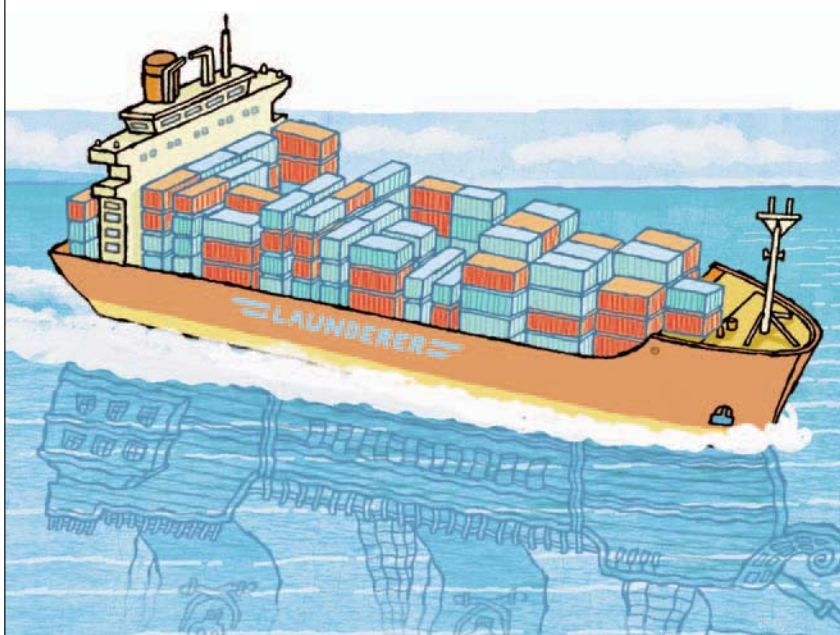
- Create a new offence for people who, or corporations which, engage in conduct that contravenes a UN sanction in force in Australia with increased penalties for breaches;
- Grant agencies responsible for administering UN sanctions lists, such as DFAT, the required information gathering powers to determine whether UN sanctions are being complied with;
- Create the offence of bribing foreign officials;
- Introduce new criminal offences for importing or exporting goods UN-sanctioned goods without valid permission; and
- Introduce a new criminal offence for providing information that is false or misleading material, or omits details, in an application for a permission to import or export UN-sanctioned goods.

Entities that discover they hold assets belonging to a UN-sanctioned entity must freeze the assets. The definition of assets under the ITIA includes property of any kind, whether tangible or intangible, movable or immovable, however acquired, as well as legal documents and financial instruments. Separate to the ITIA, reporting entities must also report any suspicion of terrorism financing to AUSTRAC within 24 hours pursuant to requirements under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act).

Joining the dots?

The Wolfsberg Group is not alone in its call for 'substantial participation from other key stakeholders' in combating TMBL, sanctions and corruption. US lawyers Ross S. Delston and Stephen C. Walls also argue that most trade-based activities happen well beyond the scrutiny of financial institutions in their recent paper, *Reaching beyond banks: how to target trade-based money laundering and terrorist financing outside the financial sector*.

most trade-based activities happen well beyond the scrutiny of financial institutions





Both the Wolfsberg paper and the paper published by Delston and Walls concur that financial institutions face significant difficulties in identifying unusual and suspicious trade-finance transactions.

It is this difficulty, they explain, combined with the scale of trade volumes that highlights the need for a holistic approach, encompassing the public and private sectors, to combating TBML and predicate crimes such as sanctions breaches and corruption. For example, TBML can be inextricably associated with certain predicate crimes that generate proceeds of crime, such as drug trafficking and human trafficking. Trade movements can disguise the logistical support for terrorist activities, such as the movement of WMD and the materials used to make them.

'Each year, more than 20 million containers enter the US by sea, rail and truck, from foreign countries, including those with porous law enforcement and regulatory regimes. Of those twenty million containers entering the US annually, fewer than five percent are physically inspected,' they state.

Twenty million containers annually mean more than 54,000 containers a day (ignoring weekends and public holidays). Delston and Walls argue that the participation from other key stakeholders could be driven via a new FATF recommendation, which would cover all entities involved in the international trade supply chain. The recommendation would require national governments that already comply with other FATF recommendations to develop legislation requiring these entities develop, implement and maintain AML/CTF programs.

In December 2008, Prime Minister Kevin Rudd admitted in his *National Security Statement*⁴ that transnational crime – such as trafficking in persons, drugs and arms; and people smuggling remained a continuing challenge both to Australia and abroad. He also noted that terrorism was likely to endure as a serious threat to Australia for the foreseeable future.

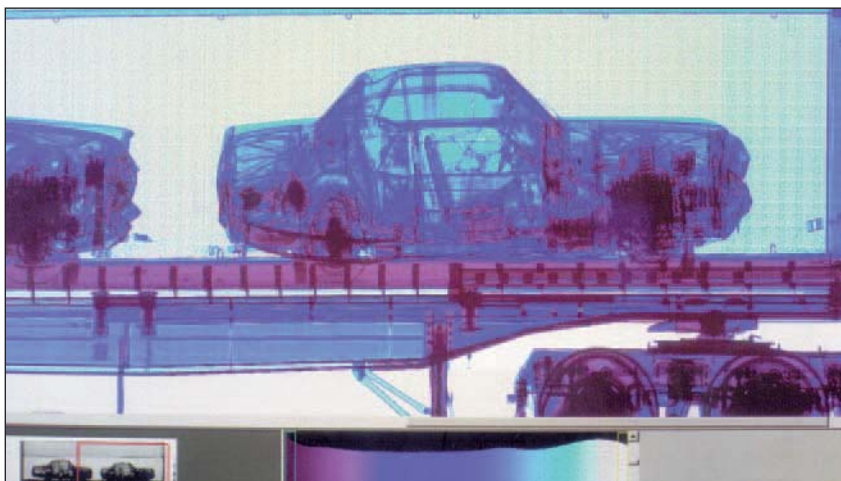
The Prime Minister also admitted, however, that while law enforcement and intelligence agencies are doing their best, Australia lacks the united front necessary for the job. He stated that '...the government has inherited ... a wide range of government agencies but lack(s) unified control and direction and a single point of accountability.'

The *National Security Statement* was used by the Prime Minister to announce a shift in Australia's response to border management and serious and organised crime. This shift, he said, will include simplifying arrangements and improving coordination across all agencies through the creation of a National Security Adviser. It also includes a 'beefed-up' ACBPS, giving it the capability '...to task and analyse intelligence, coordinate surveillance and on-water response, and engage internationally with source and transit countries to comprehensively address and deter people smuggling throughout the operating pipeline from source countries to our shores.'

The *National Security Statement* confirms that the efforts to combat TBML, sanctions and corruption within Australia are largely

the participation of industry groups involved in international trade and transport.

Frontline members sign a memorandum of understanding (MOU) to formalise this cooperation; receive training on illegal drugs and activities; and undertake to report suspicious activity linked to air and sea cargo and persons of interest to the ACBPS Frontline hotline. However, while reporting entities have a legislative obligation under the AML/CTF Act to identify and mitigate ML/TF risk, identify their customers and report suspicious matters, international trade and transport entities volunteer to join the Frontline program and mark their participation by signing non-contractual, non-legally binding MOUs to report suspicious activities. They are not subject to



X-RAY SCAN OF CAR CONTAINER

unlinked and unregulated, apart from reporting entities covered by the AML/CTF Act.

The ITIA for instance, applies to *all* corporations, not just financial institutions. It requires all persons who apply for a licence, permission, consent, authorisation or approval under a UN sanction enforcement law to keep records of the application and records demonstrating their compliance with any conditions to which the relevant authorisation is subject for five years. However, compliance with the legislation is currently unregulated and, while the Australian Bankers Association has plans to release guidance around the Act, it will only apply to the finance sector. There does not appear to be any guidance being developed by other sectors such as shipping, postal and courier services or the high-risk sectors that manufacture goods capable of being used in weapons of mass destruction (a broad spectrum of businesses).

Another example where TBML regulation could be introduced is the Frontline program. Frontline is run by the ACBPS and includes

these mandatory obligations to assess and mitigate risk, to identify customers or to undertake ongoing customer due diligence or complete mandatory reporting.

For now it seems, financial institutions continue to be the first line of defence in combating TBML, sanctions breaches and corruption and without an additional FATF Recommendation Australia is a very long way from taking legislative steps to bring the many players in the movement of goods across Australia's border under the AML/CTF regulatory umbrella. And while the government may have good intentions with its new security framework initiatives, whether these will assist to spread the burden and improve the chances of reducing ML/TF risk associated with trade movements remains to be seen. □

Emily Brayshaw (CAMS) (Dip Intl. AML) is an independent AML/CTF contractor and trainer with more than five years experience in the field in Australia and abroad. She may be reached at emily.brayshaw@iinet.net.au.

4 See http://www.pm.gov.au/media/Speech/2008/speech_0659.cfm for a full text of this statement.