Old Laundering Methods Hold Fast

Cash smuggling and trade-based money laundering continue to be favourites with money launderers and now even terrorist financiers. Rohan Bedi explains.

While banks have traditionally focused on cash deposits, controls on trade laundering have not been as good. Moreover, the dimensions around cash laundering need to be understood better. This article will focus on Hong Kong and linked laundering from China.

Cash-Based Laundering

Cross-border bulk cash smuggling can be in either currency or monetary instruments (bearer; TCs; ‘pay to the order of’). Bulk cash smuggling is typically via couriers (‘mules’) who travel on a flight/ship. For larger operations, charter planes/ships/trucks are used – third party or owned by the launderers through shell companies.

Alternately, underground banking (called ‘fei ch’ien’ or ‘hawala’), is a popular method for moving funds cross-border, e.g., from China to Hong Kong. Money services businesses (MSBs) set up for short periods of time (e.g. 3 months) or bought out are also misused. Moving money using prepaid and stored value cards (e-money on chips) is another alternative. Smuggling of goods cross-border e.g. of pirated optical discs from China to Hong Kong is also popular - these are then sold and the cash placed into banks through a front business.

Regulations

In October 2004, the FATF released Special Recommendation nine on Cash Couriers (for anti-terrorist financing) that requires a declaration system for cross border movements of cash with border/customs officials having the power to confiscate and punish. China’s laws prohibit passengers from carrying more than RMB 20,000 yuan (approximately US$2,500) or, in foreign currency, up to US$5,000, in or out of the country on each trip. There has been a huge spike recently in cash smuggled across the border between China and Hong Kong. Offenders are fined and where the amounts are large the money is seized.
The US International Narcotics Control Strategy Report (INCSR) 2007 states that Hong Kong is deliberating ways of complying with FATF Special Recommendation Nine but does not intend to put in place the recommended "declaration system". Law enforcement agents in Hong Kong are already empowered to seize criminal proceeds at any place, including at the border. Hong Kong banks have been permitted increases in the scope of RMB business they can offer to clients. Hence many financial transactions related to China have been brought out of the money-transfer industry and into the more highly regulated banking industry, which is better equipped to guard against money laundering. Nonetheless, the report adds that new provisions allowing the use of RMB in Hong Kong have also created new loopholes for money laundering activity.

**Placement of Cash**

Once the cash is moved into another country, it can be placed in banks using for example:

- **Cash-intensive front businesses**, like restaurants or convenience stores, which mix proceeds from genuine business with illegitimate income, which is normally spread out to attract minimal attention.

- **Offshore Companies**. These can be shell companies that exist only on paper (including shelf or pre-incorporated companies) and are used to impersonate as an operating business. Alternately, offshore companies can be used to own the front business directly or through owing a locally incorporated firm. Offshore companies provide a degree of anonymity given the high levels of corporate and banking secrecy, especially where bearer shares, nominees and trusts are involved.

- **Lawyer-Client accounts**. This is another favourite for cash placements because of the credibility attached to a lawyer's name. This is especially true where lawyers are not regulated for AML and are protected by lawyer-client professional privilege. The monies could be used to pay the down payment and instalments on a mortgage enabling a smooth movement into the layering stage.

- **Accountant-client accounts and more generally services** of accountants have also been repeatedly abused by money launderers, sometimes as accomplices but often unknowingly for their professional services. Accountants also have professional privilege in many jurisdictions.

**Hong Kong Companies**

There is no "offshore company" legislation in Hong Kong and companies are incorporated under the HK Company Ordinance, 1997 version, as amended 2004. If a Hong Kong company does no
business in Hong Kong and derives no income from Hong Kong sources, then it is not taxable in Hong Kong. Also, Hong Kong’s financial regulatory regimes are applicable to residents and non-residents alike.

The crime situation is significant in both China and Hong Kong. Major laundering cases include for IPR Theft. The International Monetary Fund estimated that money laundering in China may total as much as US$24 billion annually. The INCSR states that Hong Kong-registered companies figure prominently in schemes to transfer corruption proceeds and in tax evasion recycling schemes in the People’s Republic of China. Proceeds of tax evasion, recycled through offshore companies, often return to China disguised as foreign investment, and as such, receive tax benefits. China’s cash-based economy facilitates the movement of monies in China. The easy availability of counterfeit identity documents from China creates additional vulnerabilities.

The INCSR highlights that Hong Kong companies are typically owned by BVI IBCs and involve nominee directors. The name of the beneficial owner is not documented as a public record; by executing a simple declaration of trust with a nominee shareholder and director, the beneficial owner can keep out of public records. Some banks rely on the vouching of the company formation agent. However, suspicious transaction reporting by professionals, including those acting as company formation agents, has been poor. A new bill will strengthen controls by trust and company service providers, professionals (lawyers, accountants), real estate agents, etc. - on beneficial ownership and source of wealth of their corporate clients, and STR filing.

Importantly, BVI IBCs have been exploited for money laundering for a long time. Although BVI has brought in controls including on bearer share companies, the registered shareholders of BVI companies could be entities from jurisdictions where unrestricted bearer shares are available - e.g., Nevis and Panama. Also, launderers may use a Panama private interest foundation to hold registered BVI bearer shares – a favourite for secrecy. Moreover, even with AML regulations, due diligence at the BVI offshore company incorporation stage is not difficult to circumvent for an experienced launderer using fraud IDs and nominees and operating through mail. Other risks include the BVI offshore company’s offshore bank account being used in layering (e.g. with placements in countries in Eastern Europe); deposits of USD cash directly through a BVI MSB (currently unregulated for AML) owned/controlled by the launderer, or through local front cash-intensive businesses bank accounts in USD.

<table>
<thead>
<tr>
<th>Cash-Based Money Laundering Key “Red Flag” Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ New accounts for offshore companies carrying on a local business, especially if incorporated in a former FATF black-listed country.</td>
</tr>
<tr>
<td>▪ Accounts used to receive or disburse large sums but show virtually no normal business-related activities, such as the payment of payrolls, invoices.</td>
</tr>
<tr>
<td>▪ Frequent exchange of small-dollar denominations (e.g. from street drug sales) for large-dollar denominations.</td>
</tr>
<tr>
<td>▪ Safe deposit box or safe custody account used very frequently.</td>
</tr>
</tbody>
</table>
Cash deposited is of large denominations (especially if wrapped in currency straps and in USD 100s -preferred for international bulk cash smuggling).

The cash deposits are matched by outflows (‘layering’) (especially if offshore/ high-risk jurisdictions) or transfers to unrelated accounts, accounts of professionals and personal accounts.

Hawala operators who run cash-intensive businesses that co-mingle funds in bank accounts and then to settle accounts, utilise trade-linked wire transfers or purchase negotiable instruments.

Deposits of sequentially numbered monetary instruments especially if bearer.

Structuring – cash and monetary instruments deposits are just below internal/ external currency transaction reporting requirements (e.g. USD 10,000).

The cash deposits are followed shortly by withdrawals overseas by ATMs.

Where allowed (e.g. Japan), frequent anonymous deposits (without using cards/ the need for any bank account or ID) via ATMs in cash to bank accounts.

Cash deposits into apparently unrelated individual accounts (“Smurfs”) which are then consolidated into one account through funds transfers.

Client purchases large numbers of cashier’s cheques and money orders with the cash deposited, especially if structured or via internet banking services.

Sudden spurt in cash deposited into an existing cash-intensive business account – could indicate change of ownership or misuse of a legitimate business account.

Certificates of Deposit are purchased which are then used as loan collateral, especially if in a cross-border loan to an offshore company.

Loan taken against the security of the cash deposited and then channelled offshore or used for a purpose other than the purpose recorded.

In addition to the above red flags, banks should watch for large numbers of prepaid and stored value card transactions using the banks services or third party online payment systems.

**Trade-Based Money Laundering**

Banks get involved through money transmission, provision of finance (LCs) and via lending the institutions name to a transaction.

False trade pricing has long been misused to launder money; avoid taxes, tariffs, and customs duties; tax fraud; capital flight; corruption; and even generate quick illegal profits (e.g. export incentives). Schemes include:

- Undervaluing exports, overvaluing imports: by invoicing below market value, the exporter transfers value to the importer, because they will get a higher price when they sell on the open market. By invoicing above market value, the exporter receives value from the importer. In government corruption schemes, the Politically Exposed Person (PEP) can facilitate the payment of over-invoiced goods and receive the proceeds of corruption separately in his/her offshore shell company.

- Multiple invoicing is used to make multiple payments for the same shipment or delivery of services via different banks.

- Fabricating shipments ie, using false invoices and other shipping documentation.
- Falsifying trade weights by overstating or understating quantity (e.g. semi-filled or empty boxes; also called ‘fresh-air invoicing’).
- Falsely describing goods and services e.g. shipping an inexpensive item described as an expensive item or an entirely different item.

Sophisticated criminals will undertake transactions which combine some of the above techniques as well as exploiting the financial system. This makes it harder to detect their activities. Invoice manipulation is also used in hawala transactions to settle books between operators.

Nonetheless, trade-based laundering does not always involve fraud. If for example, USD 100,000 needs to be remitted and the terrorist financier does not want to attract attention, it’s easier done by exporting goods from a legitimate company to another using a genuine invoice. The goods can then be sold locally and the monies used.

From a macro customs perspective, trade data can give insights to laundering schemes where, for example, imports of a commodity (e.g. Gold) from a country are far beyond that country’s production capability. Customs officials should also remember that criminals are fairly happy to pay higher customs duties to get their goods through.

The Black Market Peso Exchange (BMPE), a trade-linked laundering system for Colombian narco-profits made primarily in the US, has used both China and Hong Kong legitimate companies and FIs to launder money. The entry of foreign banks in China will increase the vulnerability of China to these sorts of suspicious transactions.

**Trade Red Flags**

Banks deal in trade documents and do not see the underlying goods. Nonetheless, they can watch for the relevant red flags and also specifically check trade pricing and for offshore shell/shelf companies.

<table>
<thead>
<tr>
<th>Trade-Based Money Laundering Key “Red Flag” Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice;</td>
</tr>
<tr>
<td>- Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped;</td>
</tr>
<tr>
<td>- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity’s fair market value;</td>
</tr>
<tr>
<td>- The size of the shipment appears inconsistent with the scale of the exporter or importer’s regular business activities;</td>
</tr>
<tr>
<td>- The type of commodity being shipped is designated as “high risk” for money laundering activities, for example, high-value, low-volume goods (e.g. consumer electronics), which have high turnover rates and present valuation difficulties;</td>
</tr>
</tbody>
</table>
The type of commodity being shipped appears inconsistent with the exporter or importer’s regular business activities;
- The shipment does not make economic sense, for example, the use of a forty-foot container to transport a small amount of relatively low-value goods;
- The commodity is shipped to (or from) a jurisdiction designated as “high risk” for money laundering activities;
- The commodity is transhipped through one or more jurisdictions for no apparent economic reason;
- The method of payment appears inconsistent with the risk characteristics of the transaction, for example, the use of an advance payment for a shipment from a new supplier in a high-risk country;
- The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction;
- The transaction involves the use of repeatedly amended or frequently extended letters of credit; and
- The transaction involves the use of front (or shell) companies.

[Source: FATF June’06 report]

Protecting Vulnerabilities – Some Tips

How can banks combat cash-based and trade-based money laundering? Through proper know your customers (KYC) processes and attention to the red flags. Banks should focus on:

Account Opening KYC
- Account opening checks for shell/shelf companies should be strong including special arrangements for verification of offshore companies and usage of a good KYC database of “bad guys”. Focus on country risk is important.
- Because of the complexities in company account opening, many banks prefer separate account opening sections independent of the sales personnel.
- Customers’ knowledge can be a key red flag. If for example, they claim to be an importer for five years, then not knowing the basics of LC transactions should hardly be acceptable.
- Casual unannounced visits to the client office during prime business hours may lead to important insights at account opening and also subsequently.
- Focus on the fact that trade in gold, diamonds, other precious metals and gems has long been associated with money laundering, terrorist financing, and hawala settlements.
- System flagging of cash-intensive and import-export businesses and also risk rating of the customer/ account based on country, business, entity, and transaction risks is an important control.

Enhanced Scrutiny
The commingling of dirty monies with the cash flows of legitimate businesses creates difficulties in detecting such laundering schemes. A sudden change in business performance vis-à-vis history or in comparison to its peers is an important red flag.
- Controls in trade finance and other operations units that collect or make trade-related payments are critical as are reviews in the transaction monitoring unit. For cash-intensive businesses, controls in the teller counters, by branch management and in the transaction monitoring unit are critical.
- Subject all new accounts to enhanced scrutiny for a period of 6 months.
- Focus on country risk (money laundering, terrorist financing, corruption) associated with trade linked transactions is important. The INCSR is an annual report and can help in this assessment as can Transparency International’s annual Corruption Perceptions Index and Bribe Payers Index (CPI/BPI).
- Reviews for PEPs and other “bad guy” status using KYC databases is important.
- Check for red flags for cash-based and trade-based laundering. For trade-based laundering, a review for documentation fraud must also be done.
- Subject high-risk accounts classified at account opening or during the life of the account to enhanced due diligence, including using third party reports where considered necessary.
- Based on the risk rating of the customer/account, periodic review of beneficial ownership is needed in addition to event based (e.g., a large transaction) reviews.
- Use the internet to facilitate trade pricing checks. Check for indicators of fraudulent valuation (such as deductible charges, insurance costs, shipping costs and methods of shipping in relation to the goods being shipped). Google Scholar can help to know more about a particular industry. A new web-based programme called the International Price Profiling System (IPPS) is available in 2007 allowing bankers to identify client abnormal trade pricing on a real-time basis. See http://www.internationaltradealert.com/
- Unusual transactions could include trade payment transactions that do not have a trade financing leg i.e., without a LC – typically only where there is an old and well established relationship or family ties – this needs verification. Banks could ask for supporting trade documentation where transactions are unusual and even check such documentation with customs departments, if necessary.
- LC-backed payments. Although they cover a bank for credit risks against advances to the exporter, money laundering risks could still exist, for example, via false trade pricing. The LC issuance itself may be backed by a cash deposit of dirty monies. Banks should also exercise prudence in case the beneficiaries of the LC or the shipping companies (shipping the goods) are owned by the bank customer who opens these letters.
- Other red flags related to LCs are if the customer makes changes to a LC beneficiary just before payment is to be made; changes the place of payment to an account in a country other than the beneficiary’s stated location; the customer’s standby letter of credit is used as a bid or performance bond without the normal reference to an underlying project or contract, or in favour of unusual beneficiaries.
- Accounts that regularly receive consultants’ fees for services rendered need enhanced scrutiny. Review if other indicators of a regular business operation are present and if the person/entity’s profile is in-line with the stated profession.
Conclusion

Hence, cash-based and trade-based schemes continue to be key in both money laundering and now also in terrorist financing operations. Banks have to enhance their existing controls to recognise the unique risks of the markets they operate in while allocating resources adequately in a manner that gives them the most marginal benefit given their legal obligations. Customs also have to tighten their controls on trade.

************************

The writer Rohan Bedi (www.rohanbedi.com) is a leading AML/CFT expert. This is his personal comment. Rohan is closely associated with ICPVTR (IDSS), Singapore.