Hanging out the dirty money laundry

Money laundering has a long, if not noble, history. **SANDRA LAWRENCE** looks at some of the more common schemes that are used.

Money laundering has always been a significant issue with financial institutions and other cash dealers, but the events of September 11 have caused it to finally gain the recognition it deserves.

For many years, cash dealers in many countries have been complacent about their responsibilities concerning suspected money laundering. Many people have the attitude that "money laundering doesn't hurt anyone", but the citizens of Nigeria, Philippines, Mexico and Nicaragua, and several other countries that have been rocked by money laundering scandals, would no doubt strongly disagree.

What is money laundering?

Money laundering involves moving money around in such a way as to disguise its origin. For many years, the term 'money laundering' was only associated with drug traffickers, who had to hide their illicit gains (also known as 'dirty money') from the police. But of course, laundering methods can be used by anyone who needs to hide illegally obtained funds.

For example, the former dictator of Nigeria, Sani Abacha, was the subject of an international money laundering scandal. His successor claimed that Abacha stole US$4 billion from the country's reserves and sent most of the money offshore. One bank alone had accepted deposits totalling US$214 million from Abacha's sons. The Nigerian Government is now desperate to recover some of the stolen money as the country's finances are in severe trouble after several years of systematic theft.

AUSTRAC

AUSTRAC is Australia's anti-money laundering regulator and specialist financial intelligence unit. Its head office is in Chatswood, Sydney.

One of the most popular methods used by criminals to launder their money is structuring. Under the Financial Transaction Reports Act, cash dealers are obliged to report all 'significant cash transactions' to AUSTRAC.

A significant cash transaction is any cash transaction involving not less than $10,000. Most criminals know they will be subject to completion of a Significant Cash Transaction Report if they conduct a cash transaction for $10,000 or more. To avoid this, they structure the transaction. That is, they will make several deposits for amounts just under $10,000. They will often use a team of people, colloquially known as smurfs, to do their running around.

If a cash dealer suspects that someone is structuring transactions, then they should submit a Suspect Transaction Report. In fact, these reports should be submitted for all suspicious transactions, not just suspected structuring.

Another popular method of money laundering is to purchase negotiable instruments such as travellers cheques and money orders. The criminal will use the dirty money to purchase several negotiable instruments, then they can simply use these instruments anywhere in the world, at their leisure.

These instruments can even be mailed to an overseas location—much easier than mailing a large amount of cash. Plus, the more times they move the money, the harder it is for the authorities to trace it.

Wire transfers are believed to be one

SANDRA LAWRENCE

of the most common methods of laundering in many countries. In 2000 there were more than $500 million in suspicious wire transfers in the US.

In Australia, cash dealers are obliged to report all international funds transfers to AUSTRAC. However, cash dealers are not obliged to identify the person who is making the international funds transfer. Therefore, a criminal can walk into a bank and arrange for a wire transfer yet they don't have to produce any identification. No wonder it is a popular method of laundering!

Another trend that is becoming apparent is the use of products such as unit trusts and securities. The liquidity of these products makes them an ideal vehicle for launderers. They can quickly move the money through the particular product/security, then transfer it somewhere else, at little cost.

This is cheaper than purchasing a product such as an investment-linked insurance policy, where you will usually be penalised for early redemption. If you purchase direct shares, you will have to pay brokerage and stamp duty, but there is no penalty for buying and selling in quick succession (unless you incur a loss on the sale). There is also less chance that the transaction will be reported to AUSTRAC.

Brokers may not realise that a client who is buying and selling in quick succession may be laundering dirty money. If you observe a transaction that seems suspicious, or is not commensurate with the client's known source of income, then you should consider submitting a Suspicious Transaction report to AUSTRAC.

There is also 'underground banking' and this type of banking has been operating in many countries for several decades. This involves a banking-like operation that is carried by unlicensed entities operating outside the conventional system. It is based on trust and contra arrangements. There is usually no paper-trail left behind.

As an example, say Jane wants to launder some money. She goes into a shop in Sydney, which on the surface may just be a dry cleaners, travel agency, or other inconspicuous set-up.

However, Jane knows that they are also operating as an underground banker or remittance agency. Jane gives them $50,000 cash and says she wants the money sent to India.

Jane is given a chit, or a code number. She then pays a small commission and leaves the shop. The shop operator will then telephone their contact in India (or send an email), telling them to pass $50,000 to a person who presents the chit, or code number that Jane was given earlier.

In the meantime, Jane has contacted her operative in India, and given them the code number or mailed the chit to them. Jane's operative goes into the shop in India and presents the chit/code number in exchange for $50,000 cash.

At no time, were any funds sent to India from Sydney. This is purely a contra arrangement, and at some time in the future, the Australian shop will do a similar deal for the shop in India. It is difficult for law enforcement and regulatory agencies to track this type of transaction. It is believed that underground banking is also used by terrorists to move their funds around the world.

Red flags of money laundering

If you work for a cash dealer and were wondering how to identify suspected money laundering, here are some of the red flags that may indicate such activity:

- Investment decisions that don't make sense, e.g. selling shares at a loss;
- Where an investment is inconsistent with the person's employment;
- Structuring of transactions, to avoid the $10,000 rule;
- Many different people conducting transactions on the one account;
- Client is always represented by a lawyer, accountant or offshore entity;
- Wire transfers made immediately after funds have been deposited;
- Frequent fund transfers made to well-known offshore havens;
- Constant recycling of funds through a loan, i.e. redrawing and making extra payments;
- Sudden repayment of a problem loan;
- Client is not concerned about paying high fees and commissions;
- Transfers (including wire transfers) involving the same originator and beneficiary, e.g. Fred Johnson sending money to Fred Johnson's other account;
- Insurance policies with values that are inconsistent with the buyer's needs;
- Purchasing or selling at prices significantly above or below market price;
- Currency exchange transactions where the customer tries to swap a large number of low denomination notes for higher denominations;
- Large cash deposits using the night-safe, so they don't have to deal with any bank staff;
- Reluctance to provide personal information when opening an account, or providing information that can't be verified.

Fraud and financial scams

There are many different types of fraud and financial scams operating around the world and it is difficult to keep up with the trends. As soon as one scheme is terminated, another seems to take its place.

Most people have heard of the Nigerian letter scam (in which some people have been arrested by the Nigerian Government) and recent pyramid schemes yet in spite of all the publicity surrounding these ventures, they are still nailing victims on a regular basis.

Identity fraud

The fraud that is probably causing the most concern at the moment is identity-related fraud. Identity fraud is where someone uses your personal details, or a fictitious identity, in order to obtain a benefit to which they are not entitled.

For instance, someone uses your name, date of birth and bank account number to ring up your bank and pretend to be you. They may even have gone through your garbage to obtain your credit card number, signature and a myriad of other personal details.

A UK survey conducted by Experian analysed the contents of about 400 household garbage bins. The study found that 40% of bins contained an entire credit or debit card number and more than 75% of these included the vital expiry date details. One bin even produced a signed blank cheque, and one produced an unused cheque book.

If you provide a cheque to someone, such as a tradesperson, then you have actually given them your account number and signature, both of which appear on the cheque. They will know your name and address, and often these details are enough to steal your identity.

There have been recent cases in Australia where the victims, who were all of retirement age, had their superannuation funds stolen. The thief used fraudulent identity documents and arranged for the release of the funds. One US victim actually had their ID grabbed when they exchanged personal details with another driver at the scene of an accident.

There are a number of ways to prevent becoming a victim of identity fraud. These include:

- Safeguard your personal information. Do not throw personal documents into the bin, either at work or home. Use a cross-cutting shredder to destroy them;
- Limit the amount of confidential information that you carry in your wallet, in case your wallet is lost or stolen;
- Do not leave blank cheques lying around, especially signed ones. A fraudster can cash them, and can also make use all of the information contained on the cheque;
- Close any dormant accounts or credit cards that you don't use;
- Never give out personal information (credit card numbers, address, date of birth etc.) over the telephone unless you initiated the call and it's to a well-known and trusted organisation;
- If you receive a pre-prepared credit card application form in the mail, make sure you shred it (if you don't use it);
- Do not allow your bank to send your new cheque book out in the mail—pick it up from the bank;
- Have a secure mailing address such as a PO Box or padlocked letter box, as thieves regularly steal cheques and other mail from letterboxes;
- Always review credit card and other financial statements as soon as you receive them, or monitor them regularly on the internet. Monitor their receipt so that you are immediately aware if you don't receive a statement around the due date (because a thief may have rung the bank and altered your mailing address for fraudulent purposes);
- Obtain regular credit reference checks to show what credit has been applied for in your name.

Employee fraud

International fraud surveys have shown that approximately 75% of fraud is committed by employees. Approximately $^1/_3$ of employee fraud is committed by management. Most employees are honest. However, if they are presented with the opportunity and motivation to commit fraud, then many cannot resist.

Justifications for fraud include:

- They are disgruntled with their work, due to missing out on promotion or perceived unfair treatment by supervisors;
- "Everyone else is doing it";
- "I work really long hours and I'm not compensated enough";
- "I did it because I could" (opportunity);
- "I just took a little bit to start with, but it got out of control".

Some employees commit fraud because they have an addiction—such as gambling or drugs. Others simply do it out of greed. There is always some sort of motivation, which is not always something that an employer can detect or prevent. However, there are many measures that employers can implement to remove the opportunity for fraud. These include:

- Conduct a fraud risk review of your controls and processes;
- Do not allow staff to share passwords and do not allow management to keep a list of everyone's USERID and password;
- Use password-protected screen savers;
- Segregation of duties—do not allow one person to perform an entire accounting function e.g. writing cheques, signing cheques and reconciling the statements;
- Regularly rotate duties—this will often detect a fraud-in-progress;
- Do not allow staff to be possessive of clients;
- Do not relax your controls just because a trusted staff member is involved in the transaction, e.g., signing of cheques;
- Implement a fraud/ethics policy that provides guidance for dealing with suspected fraud;
- Treat all instances of fraud seriously; don't just brush it under the carpet. (Section 16 of the Crimes Act 1900 [NSW] places an obligation on persons to report serious indictable offences to a member of the New South Wales Police Force);
- Ensure that all I.T. operations have audit logs (to ascertain who was responsible for entries); data should also be backed-up regularly, to maintain the audit trail;
- Adequate pre-employment screening: how well do you check your employees before you hire them?
- Appropriate authorisation limits;
- Strict controls over corporate credit cards—insist on receipts for all purchases and thoroughly check monthly statements before signing off.

There are a number of warnings signs that may alert you to employee fraud. These include:

- Staff who never take leave and seem possessive of their office phone and clients;
- Staff who are living beyond their means;
- Sudden changes in lifestyle;
- Rumours and tip-offs;
- Unusual transactions with related parties;
- Staff who place pressure on other staff to perform a function in a non-standard way, e.g. authorising a cheque payment or bank withdrawal without adhering to correct procedures;
- Reconciliation discrepancies.

Securities fraud

Securities fraud usually relates to fraud involving debt and equity instruments, such as bonds and shares. These frauds often involve some sort of identity theft.

In one case, an insurance policyholder was entitled to receive shares after the insurance company had demutualised and listed on the ASX. However, she had not been aware of her entitlement and a male relative impersonated her, received the shares, then sold them through a broker.

The male relative had a different surname to his female victim and it seemed extraordinary that the broker allowed him to sell the shares.

Financial institutions and brokers should always ensure that they thoroughly check the identity of a customer, especially one that is not personally known to them.

Customers who only conduct transactions on the internet should be identified correctly at the time they open the account. Institutions and brokers who are cash dealers must comply with the account-opening procedures outlined in the Financial Transaction Reports Act.

Another securities fraud that has deprived numerous Australians of their savings is 'boiler room' or 'cold-calling' fraud. This scam usually involves a call from someone you have never heard of before. The caller sounds very professional and is obviously a very experienced salesman.

The caller offers to sell international securities at a "bargain, one-off" price that is "never to be repeated". Being cautious you probably ask the caller to send details. The details are eventually sent. The caller keeps ringing and eventually you succumb to the pressure and send off a cheque for $25,000. Later you receive documents purporting to be share certificates and receipts. You continue to buy and sell shares through this caller, until you have a paper profit of say approximately $200,000. However, by this time, you have sent off cheques totalling $88,000. You then decide to cash in the portfolio and ring the salesman.

Unfortunately, the phone number had been disconnected, their website is gone—they seemed to have disappeared into thin air. This was obviously a cold-calling scam, and is based on an actual incident.

Boiler room is the name used to describe the environment in which these cold-calling salespeople work. (A racket was recently exposed in Thailand.)

Some of the salespeople involved have actually been Australian tourists. It is believed that they work in very torrid, back-breaking conditions—hence the term 'boiler room'.

To avoid becoming a victim of these types of scams, always remember the adage: if it sounds too good to be true, it probably is. J

In December 2003 the Attorney General's Department published a suite of issues papers on proposed anti-money laundering reforms. The proposals relate to how the Government intends to implement the revised Financial Action Task Force (FATF) Forty Recommendations in Australia. The Securities Institute is currently working on its response to the issues paper that relates to the financial services sector.

Continued from page 36

for differences in FoF portfolios on the basis of size of assets invested. In addition, wholesale superannuation funds were reported to average eight mandates (overall) in the Rainmaker Mandate Analysis 2001.[4]

An important caveat of this study is that the costs of increasing the number of funds in the portfolio have not been considered. Investors must acknowledge that differing economies of scale will apply to FoFs of varying asset sizes, where costs relate to the administrative, search, review and transaction elements. These issues are also being examined in future research.

Acknowledgements

The authors are grateful to Mercer Investment Consulting (for continued research support) and to the Securities Industry Research Centre of Asia-Pacific (SIRCA).

References

Amin, G., Kat, H. (2002), Portfolios of Hedge Funds, What Investors Really Invest In, Working Paper, University of Reading

Bird, R., Gallagher, D. (2002), The Evaluation of Active Manager Returns in a Non-Symmetrical Environment, Journal of Asset Management, Vol. 2(4), pp303-324

Lhabitant, F., Learned, M. (2002), Hedge Fund Diversification: How Much is Enough?, Working Paper, The American Graduate School of International Management

O'Neal, E. (1997), How Many Mutual Funds Constitute a Diversified Mutual Fund Portfolio?, Financial Analysts Journal, Vol. 53(2): pp37-46.

Park, J., Staum, J. (1998), Fund of Funds Diversification: How Much is Enough?, Journal of Alternative Investments, Vol. 1: pp39-42.

Brands, S., Gallagher, D. (2003), Portfolio Selection, Diversification and Fund-of-Funds, Working Paper, The University of New South Wales.

1 ASSIRT Market Share Report, March Quarter 2002

2 ASSIRT Market Share Report March 2003; ASSIRT Market Share Reports – March 1997 and March 2002

3 Four factor alpha accounts for market, size, book-to-market and momentum factors

4 For comparison purposes, Rainmaker Distribution Platforms Report 2002 indicates that FoFs employ an average of 15 fund managers. J