

The Global Standard

This article analyses the final changes to the Financial Action Task Force (FATF) 40 recommendations incorporating important points raised by industry bodies during the consultation process.

The revised Financial Action Task Force (FATF) 40 recommendations, published in June 2003, now apply not only to money laundering but also to terrorist financing. The new recommendations advocate a risk-based approach to anti-money laundering (AML) and provide details on the customer due diligence process. They also clarify the standard of suspicious activity reporting and provide details on three key risk areas - politically exposed persons (PEPs), correspondent banking and non-face-to-face businesses. In addition, the recommendations create higher standards of transparency linked to beneficial ownership, bring non-financial businesses and professions, including lawyers and accountants, explicitly into the AML loop, and advocate a higher standard of international cooperation.

The new FATF 40 significantly affects existing AML laws and will keep governments, enforcement and supervisors busy in fully implementing the changes - both legislative amendments and new administrative arrangements. This article highlights the important new points.



The Money Laundering Offence Recommendation 1

The revised FATF 40 recommendations require that, at a minimum, each country should incorporate a range of predicate offences within

each of 20 designated categories. The list of 20 includes terrorism and terrorist financing, corruption and bribery, fraud, smuggling, insider trading and market manipulation. This is only a minimum list as it is the intention of the FATF to make AML legislation cover the proceeds of drug trafficking and all

serious crimes. The more the predicate crimes listed in a country's legislation, the better the ability to prosecute.

Predicate offences for money laundering should extend to cover offences that occur in another country. Foreign predicate offences should be as wide as the domestic predicates.

**Focus on
PEPs,
Correspondent
banking, Non-
face-to-face
Business**

Tax evasion is not stated explicitly in the list of 20 predicate crimes although recommendation

FATF 40 REVISION

13 highlights the importance of reporting suspicious transactions to avoid money launderers classifying their transactions as 'tax matters', and recommendation 40 talks of requirements for mutual legal assistance in criminal matters treaty (MLAT)-based co-operation on fiscal issues (such as foreign tax evasion). The UK goes a step further and recognizes domestic and foreign tax evasion as a predicate crime for money laundering.

Customer Due Diligence Recommendation 5

This is the most important recommendation. It defines customer due diligence (CDD) for financial institutions (FIs), with reference (during the consultation process) to the Basel Committee on Banking Supervision's October 2001 paper, Guidance on Customer Due Diligence for Banks, although the Basel paper actually goes beyond the FATF 40 recommendations. However, the new FATF 40 is more risk-based. The requirements apply to all new and existing customers on the basis of materiality and risk, and state that financial institutions should conduct due diligence at appropriate times. This includes periodic reviews and following significant customer events (such as if an existing customer opens a new account or takes out a new product). Best practice suggests that updated information obtained through any meetings, discussions or other communication with the customer should be kept.

The recommendation highlights the CDD requirements for occasional customers of FIs, and states that due diligence - such as identifying and verifying the identity of the customers - is required wherever there is a suspicion of money laundering or terrorist financing. The CDD measures outlined in the recommendations do not imply that FIs have to

repeatedly identify and verify the identity of each customer every time that customer conducts a transaction. Rather, an institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information.

The recommendation also lays down the measures to be taken with respect to existing customers and for legal persons (for example, private limited companies) or legal arrangements (such as trusts). It requires FIs to identify the identity of the beneficial owners by forming an understanding of the ownership and control structure and taking reasonable measures to verify the identity of such persons.

**Understand
the ownership
and control
structure**

If CDD cannot be done and an account is not opened, the transaction is not done or the relationship is terminated, the FI should consider filing a suspicious transaction report (STR).

**Cant do CDD
& terminate
relationship –
then consider
STR filing**

In addition to the fundamental obligations, it also deals with other issues such as the timing of verification. It is permissible under certain circumstances, where it is essential not to interrupt the normal conduct of business, for verification to be completed after the establishment of the business relationship. Examples include non-face-to-face business, securities transactions and life insurance business. For instance, for non-face-to-face business, FIs can accept the first transaction, perform verification and then allow other transactions.

FATF 40 REVISION

Financial institutions will need to adopt risk management procedures with respect to the conditions under which a customer may utilize the business relationship prior to verification. FIs should refer to the Basel CDD paper (section 2.2.6) for specific guidance on examples of risk management measures for non-face-to-face business.

The new FATF 40 advocates a risk-based approach to AML. There are circumstances where the risk of money laundering or terrorist financing is lower (by reference to the risk for that customer, transaction or product type), where information on the identity of the customer and of the beneficial owner is publicly available, or where adequate checks and controls exist elsewhere in national systems. In these circumstances, countries may decide that FIs can apply reduced or simplified measures.

Examples of customers where simplified or reduced CDD measures could apply are:

- where FIs are subject to requirements to combat money laundering and, terrorist financing consistent with the FATF recommendations and are supervised for compliance with those controls;
- where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company;
- government administrations or enterprises; and
- simplified or reduced CDD measures could also apply to the beneficial owners of

pooled accounts held by designated non-financial businesses or professions, provided that those businesses or professions are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are subject to effective systems for monitoring and ensuring their compliance with those requirements.

Simplified CDD or reduced measures could also be acceptable for various types of products or transactions, and the new FATF gives examples linked to insurance, pensions, superannuation

Simplified or reduced CDD measures can be adopted for lower risk categories

or similar schemes.



Countries could also decide whether FIs could apply these simplified measures only to customers in its own jurisdiction or allow them for customers from any other jurisdiction. Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or specific higher-risk scenarios apply.

In its comments to the consultation report, the Wolfsberg group pointed out that certain transactions or activities have a minimal risk of money laundering or terrorist financing. They give some examples:

- transactions where a financial is acting as a principal rather than on behalf of third-parties (such as foreign exchange,

FATF 40 REVISION

derivatives, capital market transactions and some extensions of credit);

- accounts established for a specific purpose with funds received or disbursed under limited defined circumstances to identified third-parties, such as escrow, corporate trusts, paying agency and custody accounts;
- accounts for the investment of funds that are subject to a regulatory scheme, such as investment of funds of regulated pension or retirement plans; and
- accounts held by other financial institutions that are themselves subject to a robust AML regime.

Politically Exposed Persons (PEPs) Recommendation 6

The FATF is concerned about the risks that FIs and financial centres face when the proceeds of corruption or abuse of public funds are routed through their organisations and centres. This recommendation discusses risk management systems and the role of senior management of FIs, among others. The glossary defines a PEP to include family members and close associates of persons who perform public functions for a state (such as head of state, senior politicians

Using good third party databases for PEP monitoring is essential

and judges), but clarifies that it is not intended to cover middle-ranking or more junior individuals. Countries are encouraged to extend the requirements of recommendation 6 to individuals who hold prominent public functions in their own country.



The Wolfsberg Group in its comments to the consultation report had pointed out that there needs to be a recognition that having PEPs as customers is not, and should not be, prohibited, but FIs will want to pay particular attention to such customers.

Correspondent Banking and Shell Banks Recommendation 7 and 18

The FATF highlights the risks of correspondent banking owing to the sheer volume of payments and the speed at which these payments must move.

Highlights role of Senior Management for PEPs and Correspondent Banking

Recommendation 7 sets out due diligence criteria, including the role of senior management of FIs. In relation to cross-border correspondent banking and other similar relationships, it lays down enhanced due diligence measures that highlight the risks of 'payable-through-accounts'

(where accounts are held at a bank by a foreign financial institution to permit its customers to engage in banking activities in that country).

Recommendation 18 adds that countries should not allow the establishment of shell banks nor allow their financial institutions to have correspondent relations with such banks either directly or indirectly via payable-through-accounts.

The Wolfsberg Group in its comments to the consultation report highlighted their new enhanced due diligence principles for correspondent banking. The principles set out

FATF 40 REVISION

risk-indicators by which FIs can assess the risks both at the inception of the relationship, and on a continuing basis, to ascertain the appropriate level of due diligence necessary to manage the identified risks. *The risk indicators include:* the domicile of the correspondent banking customer; the ownership and management structure of the correspondent banking customer; and the correspondent banking customer's business and customer base.

Electronic and other Non-face-to-face Financial Services Recommendation 8

The FATF believes that internet institutions may attract non-resident customers wanting to take advantage of the potential lack of transparency in automated transaction processing and other aspects of non face-to-face financial services.

As in-the previous FATF 40, recommendation 8 requires that FIs should pay special attention to new technologies that favour anonymity, that is, non-face-to-face relationships. Annex 1 of the consultation report lists possible measures to manage money laundering risk. It is important to note that the requirement of face-to-face verification for all new customers (measure 2) to ascertain their identity has been rejected by the British Bankers' Association and the Wolfsberg Group of Banks (a group of 11 international banks that co-operate on anti-money laundering issues). These industry groups believe that online financial services per se do not present new specific risks of money laundering, beyond the risks applicable to all non-face-to-face relationships, provided full due diligence checks are applied. Specifically, they do not lead to greater anonymity during account opening; *electronic verification and ongoing monitoring can be more vigorous and effective* (particularly because of the ease with

which many documents can be forged or obtained illegally).

Third-party CDD Recommendation 9

The new FATF 40 allows third parties to perform certain elements of the CDD process (identification and verification of customer/beneficial owner and obtaining information on the purpose and intended nature of the business relationship) or to introduce business - provided that the ultimate responsibility for customer identification and verification remains with the FI relying on the third party. The responsibility for conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship, is that of the FI.

While this recommendation does not cover agent relationships, it does extend to other types of intermediaries who may process business or perform CDD for financial sector businesses, such as 'Acceptable Referees' (as defined in local regulations – for example in Australia) whose written reference is taken to confirm the identity of the applicant customer. It covers situations like for example executing brokers and affiliated banks or clearing brokers. The recommendation does not apply to outsourcing or agency relationships, where the ultimate responsibility remains on the institution; upfront due diligence on the third party is required especially for outsourcing arrangements where periodic independent reviews of the arrangement are also required. This recommendation also does not apply to relationships, accounts or transactions between FIs on behalf of their clients. Those relationships are addressed by recommendations 5 and 7.

FATF 40 REVISION

Suspicious Transaction Reporting Recommendation 13

The FATF requires mandatory STR for proceeds of a criminal activity and to funds related to terrorist financing. All suspicious transactions including attempted transactions should be reported regardless of the amount of the transaction. The recommendation specifies that there must be a 'direct legal requirement to report', and states clearly that reasonable grounds to suspect is now the explicit standard for STR purposes.

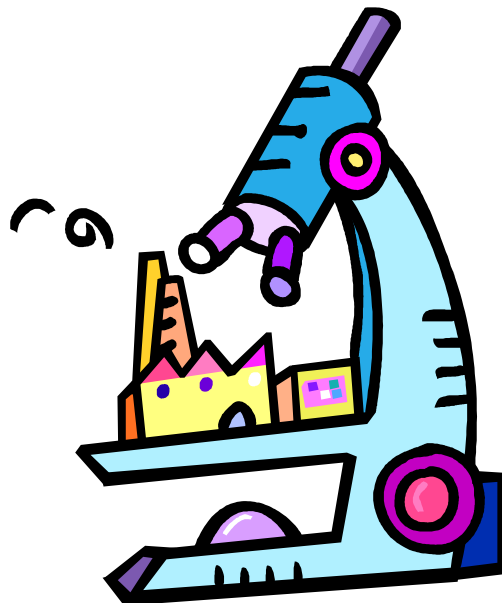
Non-transactional behaviour also needs to be monitored – for example, a change in address needs to be checked for identity theft, especially if it is repeated after a few weeks.

Tipping Off Recommendation 14

As in the previous FATF 40, the new recommendations require laws to give protection to those filing STRs and to prevent tipping off of the customer that an STR or related information is being reported. It now clarifies that if the institution reasonably believes that performing the CDD process will tip off the customer or potential customer on a possible STR investigation, it may choose not to pursue that process, and should file a STR.

Can postpone CDD to avoid tipping-off but should file a STR

The interpretative note clarifies that where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.



Regulation and Supervision Recommendations 23-25

All countries need adequate measures to ensure that FIs and other businesses and professions are complying with their obligations. The required measures take into account the risks and the regulatory structures that already exist in the relevant sectors.

The required measures are:

(i) FIs and casinos should not be owned or managed by criminals; (ii) the regulatory and supervisory measures applicable to banks, insurance and securities firms for prudential purposes also apply to them when combating money laundering and terrorist financing; (iii) bureaux de change and money remittance businesses must at a minimum be licensed or registered, and monitored for compliance; (iv) other FIs should be regulated and subject to supervision or oversight having regard to the risk of money laundering or terrorist financing; (v) casinos must be licensed and supervised; and (vi) on a risk-sensitive basis, other businesses and professions must have effective systems for monitoring and ensuring compliance, which could either be by a government authority or by a self-regulatory Organisation. In addition, competent authorities

FATF 40 REVISION

must establish guidelines and provide feedback to assist financial institutions and designated non-financial businesses and professions.

Institutional Measures Recommendations 26-32

The recommendations require countries to establish financial intelligence units (FIUs) - government units created explicitly to monitor money laundering - that will receive STRs, and to consider membership of the Egmont Group of FIUs, an organisation aimed at promoting co-operation between various FIUs. The FIUs should provide feedback on STRs and other information - the Hong Kong FIU is a good example of this in Asia. The recommendations draw attention to the Egmont Group principles for exchange of information between FIUs for money laundering cases.

The recommendations require countries to designate law enforcement agencies for AML/CFT investigations, and for financial supervisors to have a role in AML/CFT. These authorities should have appropriate duties and powers, the necessary resources, and effective mechanisms to co-operate and co-ordinate. To ensure systems are effective and that this can be reviewed, comprehensive AML/CFT statistics must be kept, for example, the number of STR received, and data on prosecutions and convictions.

Non-financial Businesses and Professions Recommendation 12

New non-financial businesses now have explicit AML requirements, such as CDD and record keeping, in specified situations. The list includes casinos (including internet casinos), real estate agents, dealers in precious metals/stones, lawyers, notaries and other independent legal professionals and

accountants (this refers to sole practitioners, partners or employed professionals within professional firms), trust and company service providers. The last category provides as one of its services 'acting as (or arranging for another person to act as) a nominee shareholder for another person'. This has been exploited repeatedly by money launderers.

Notably, advisers or entities that only provide investment advice and which do not themselves handle client funds, have been left out of the final list of such businesses on which AML obligations are explicitly recommended.

**Non-financial
Businesses and
Professions
now have
explicit AML
requirements**

Also, lawyers and accountants offering investment advice are only covered by AML requirements for 'managing of client money, securities or other assets', which does not cover advising on investments. However, FIs are covered by AML requirements including providing various investment services for a client, whereby the FI handles and invests the client's money or funds. This could extend to the provision of investment advice, where this is linked to the adviser handling client funds.

However, recommendation 16 states that STRs for all the above non financial businesses are subject to certain qualifications made. For example, particular professionals are exempted from reporting where legal professional privilege or professional secrecy applies, and accountants are required to report for specified situations outlined in recommendation 12 and strongly encouraged for other activities including auditing.

Meanwhile, recommendation 20 suggests that countries consider applying FATF 40 to businesses and professions other than

designated ones above, if they pose a money laundering or terrorist financing risk.

Corporate Vehicles Recommendations 33-34

One of the objectives of the consultation process was to deal with the risk of nominee shareholders and directors where the beneficial owner is someone engaged in illegal activities. The recommendations require countries to ensure that for legal persons, bearer shares and legal arrangements, measures are taken to facilitate financial institution access to information relating to beneficial ownership and control. In particular, countries must be able to show that companies issuing bearer shares cannot be misused for money laundering.

Private limited companies

In its response to the consultation report the British Bankers Association (BBA) said that the requirement that care should be taken to verify the identity of principal beneficial owners/controllers at account opening/ during the life of the account, is difficult for all banks to achieve, whether the corporate is in the UK or overseas. There was no present regulatory requirement on private limited companies to advise its bank of any change in beneficial ownership. The BBA said that the onus should be on regulatory/supervisory functions to make sure that there is a proper framework in place at company formation stage and whenever changes in structure take place. They say that at the most banks can be expected to take reasonable steps to consider whether the information appears correct.

Trusts and bearer shares

In its response to the consultation report the Wolfsberg Group commented that requiring the registration of trusts/ bearer shares would represent a radical change to the current procedures and would not manage the risks of money laundering and terrorist financing.

The BBA commented that they accepted that the nature and operation of trusts may not always be transparent, but state that in the overwhelming majority of cases they are established and operated for legitimate reasons and fail to pose a money laundering risk. There are certain areas of trust business that constitutes a significant money laundering risk. For instance, protection trusts and employing trusts in certain countries to escape judicial decisions to freeze, seize or confiscate assets, may well pose an increased risk. However there are many other areas of trust business dealing with normal family activities that are relatively low risk. The BBA believes that know your customer for trusts should be dealt with on a risk based approach depending upon the nature of the trust, the legal framework within a jurisdiction and the extent of the assets involved.

International Cooperation Recommendations 35-40

Several of the recommendations in the international co-operation section have been developed and refined, with recommendation 36 on mutual legal assistance being expanded to cover several concepts that are in the 25 non-cooperative countries and territories (NCCT) criteria. The most significant addition is

**Spontaneous
or upon
request
information
exchange
between
countries**

FATF 40 REVISION

recommendation 40, which deals with international co-operation other than mutual legal assistance and extradition - for example, co-operation between administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including FIUs. This prescribes the need for the widest possible co-operation and for clear and effective gateways amounting to a spontaneous or upon request information exchange via MLATs including fiscal information.



Impact on Asia

The impact on Asia is significant considering that Asian FIs are lagging behind their US/UK counterparts in many respects.

Predicate Crimes

- FIs should note the list of 20 minimum predicate offences for money laundering.

Reporting Standard

- FIs in countries that have not adopted the reporting standards 'direct legal requirement to report' and 'reasonable grounds to suspect' need to retrain their staff to meet the required standards.

CDD Processes

- FIs should review their CDD processes to ensure compliance with the now explicit definition of the process. There is a focus to not only know customers, but to also understand their businesses. In the US, for example, false trade pricing and weights have been used to launder money and evade millions of dollars in taxes.

- If CDD is not done and the transaction is terminated FIs should consider filing a STR.
- If a FI reasonably believes that CDD will cause tipping off, it may choose not to follow the process and file a STR.
- FIs can complete verification after the establishment of the business relationship in certain situations.
- FIs should adopt a risk-based approach to AML. This allows simplified CDD in certain situations. This also requires greater due diligence on high-risk products and customers: gather more and better information. 'Know Your

Customer' formats should be up to date, and reflect best practice guidance such as the Wolfsberg principles.

- FIs should note the role of senior management for PEPs and correspondent banking accounts.
- FIs should note the requirements for third-party CDD.
- FIs have a heightened responsibility to be vigilant in monitoring for beneficial ownership information (both at account opening and during the life of an account) given the new requirements for better institutional availability of such information. Greater corporate transparency brings focus on identifying the beneficial owners of private limited companies, bearer share companies and trusts.

Highlights risk of nominee relationships/ requires more institutional recording of beneficial ownership information

FATF 40 REVISION

- The USA PATRIOT Act highlights a whole host of non-documentary verification methods that should be used as part of CDD procedures. These include negative verification (fraud and bad-check databases), positive verification (credit reports), logical verification (identifying if information is logically consistent) and more.
- FIs who accept accounts for the high-risk non-financial business that are now to be regulated for AML purposes, should ideally review the quality of the AML programs of the firm opening an account, as is best practice for other FI accounts.
- More generally, sanctions of other countries can also have an impact. For example, transactions with a US bank that have a hit on the US Treasury Office of Foreign Assets Control (OFAC) blacklist, which includes names of terrorists and other bad guys including black-listed countries, can block transactions. Transactions may also be rejected instead of blocked.

Politically Exposed Persons

- The PEP threat is very apparent from the Transparency International Corruption Perception Index (CPI) 2005 listing of many Asian countries with poor CPI scores. Ownership of the risk assessment process by the Relationship Managers is critical, especially in the Private Banking business.

Correspondent Banking

- Correspondent banking is the 'great unknown', which is a problem area that almost all FIs will have to address – in terms of knowledge levels and in terms of processes. The USA PATRIOT Act also highlights the importance of this business and underscores the new 'extra-territorial' impact of foreign regulations. For Asian FIs having a correspondent account with a US

FI, it has created new information, due diligence and reporting requirements. Laundered monies in bank accounts of an Asian bank outside the US can be confiscated from its correspondent banking account in the US. Non-compliance can lead to fines even if there is no clear money laundering case. In the worst case scenario account closure is possible. Use of a US FI outside the US to launder money is now deemed 'conduct' in the US.

Non-face-to-face Business

- FIs should review the money laundering risk in their non-face-to-face businesses and reflect it in their CDD and transaction monitoring systems.

Funds Transfers

- FIs funds transfer manual and system processes should be compliant with Special Recommendation 7 and the interpretative note covering both cross-border and domestic transfers between FIs. This increases originator information, such as name, account number (if there is an account, otherwise a unique reference number), address (or suitable replacement - a national identity number, customer identification number, or date and place of birth) on all funds transfers (domestic/cross-border) and requires financial institutions in chain transfers to keep all originator information with the transfer. SWIFT's new format the MT103, implements the FATF requirement for more detailed information and has been adopted by banks. Due diligence required on funds transfers for CFT purposes has been enhanced as a result of the enhanced availability of information.

FATF 40 REVISION

Transaction Monitoring

- FIs need to identify and flag high-risk businesses such as money managers, money services businesses (high risk for terrorist financing), cash-intensive businesses, and PEPs, and subject these accounts to enhanced monitoring and independent testing by internal audit i.e., a process of enhanced due diligence. Transaction monitoring software is critical for this process. Our experience in Asia tells us that this is an area that has serious weaknesses.
- It is also advisable to flag and monitor non-resident accounts from high tax evasion Asian countries, owing to the growing trend in international exchange of information, for example in the European Union.
- Those FIs that have online businesses such as internet broking or internet banking will be expected to have effective AML transaction monitoring software in place. This is expensive and needs budgets to be approved.
- Combating the Financing of Terrorism is a key new requirement for which FIs need to buy into 'bad guy' data-bases to monitor. Focus on non-profit organizations and cash-intensive businesses, is also required. The latter is because terrorist financiers are increasingly indulging in criminal activities to generate monies and need to launder these monies (other typologies include trade laundering schemes). Rich individuals have also been known to finance terrorism. Money Services Businesses (MSBs) have been involved in counterfeit cheque schemes that help terrorists and non-governmental charitable organisations that use MSBs to transfer proceeds out of the country. Unregistered MSBs (Hawalas) are used by terrorists to transfer monies.
- FIs will also need to look seriously at PEP databases (such as Factiva and World-Check) to ensure that proper transaction

monitoring is happening in private banking and correspondent banking etc. PEPs from certain countries have also been known to have links with terrorists.

Training & Awareness

- Asian FIs should ensure money laundering identification and enquiry skills, supported by training programs that benefit from e-learning techniques, case study applications, video, audio and role plays. Focus on internal audit to upgrade their skills is essential.
- Awareness measures through newsletter subscription by compliance/ internal audit and focused ongoing dissemination to front-office staff of case-studies, articles and relevant desk-based guidance, as well as pointed senior management messages on the importance of AML/CFT – this is all critical.

Senior Managements Role

- The US/UK culture of fines and 'name and shame' will eventually catch up with Asia. Already, in Asia's financial centers strong letters from the supervisor on AML/CFT lapses are being sent out to the branches head offices. This underscores a new supervisory approach to enforce the personal accountability of senior management for adherence to regulatory requirements that is typically enshrined in the banking or AML/CFT acts. Needless to say head offices do not react mildly to such letters.
- In line with global best practices, the AML/CFT program should be developed based on the boards' risk tolerance levels and should be board-approved. As part of this process, boards also need to approve the customer identification program.

FATF 40 REVISION

- In addition, senior management needs to update the customer identification program on an ongoing basis.
- There is also a trend toward global cooperation for AML, which means new risks for businesses that rely on flight capital. This issue needs to be considered.

Conclusion

Compliance with the new AML/CFT requirements is more than a regulatory compliance issue; it is a broader enterprise-wide risk management issue. A leading US Money Services Business earlier paid a fine of US\$8 million for poor AML controls, while an Asian bank was fined US\$20 million for poor controls in its New York branch. Fines have now sky rocketed to US\$100 million. Equally important are the issues of reputation loss, loss of stakeholder confidence, and the potential for negative impact on share price.

Do other Asian FIs want to go down this painful and expensive route? If not, an appreciation for this fact or 'tone at the top' must be reflected in budgets for AML/CFT systems.

[Updated February 2006 version of articles first published in *AsiaRisk* magazine in September 2003 ('The Global Standard') and April 2003 ('Widening the net'), *Bangkok Post* in October 2003 & February 2003, and *Manila Times/Business Times* in March 2003.



Written originally by Rohan Bedi as Head of AML Services, PricewaterhouseCoopers Singapore.

Email: rohanbedi@rohanbedi.com