David Carse: Anti-money laundering and the role of supervision

Speech by Mr David Carse, Deputy Chief Executive of the Hong Kong Monetary Authority, at the Hong Kong Institute of Bankers, Hong Kong, 23 August 2002.

* * *

Ladies and Gentlemen,

Introduction

I welcome the opportunity to talk to the Institute on the subject of the fight against money laundering and the role that supervision plays in this. This is a good time to speak on this subject since we are currently reviewing our 1997 anti-money laundering guideline in the light of the latest developments in this area. I will use this speech to highlight some of the issues that we are addressing.

It is also a useful occasion for me to remind the bankers gathered here today how important it is to combat money laundering. This should really go without saying and I do not intend to dwell on it too much. The key message is that authorized institutions ("AIs") should view anti-money laundering systems as an essential means of self-preservation - and not as a nuisance or an unnecessary expense that is imposed upon them.

The events of 9/11 have heightened the international concern about money laundering. There is less and less patience with jurisdictions, and their banks, that do not comply with the international standards laid down by bodies like the Financial Action Task Force ("FATF"). The FATF has begun to "name and shame" jurisdictions that it regards as non-cooperative countries and territories ("NCCTs") in tackling money laundering. Such NCCTs will be subject to sanctions if they do not come into line.

Moreover, banks from NCCTs are caught under the newly enacted US Patriot Act. Such banks, and any others regarded as higher risk from a money laundering perspective, will be subject to increased scrutiny by their US correspondent banks and the US authorities. At worst, higher risk foreign banks could eventually find themselves shut out of the US payments system.

Hong Kong has a good reputation internationally as a financial centre that takes seriously the need to combat money laundering. I am sure that you will agree that we all have a vested interest in keeping it that way - which means that we need to keep in line with international standards as they evolve.

The role of the HKMA

The role of the HKMA in this is to work with the other relevant authorities in Hong Kong - the Commissioner for Narcotics, the law enforcers and other regulators - to ensure that we have an effective framework to deter, detect and report cases of money laundering. Our particular responsibility relates to AIs. It is our job to verify that AIs have adequate policies, procedures and controls in place to enable them to:

- identify suspicious customers and transactions;
- report suspicious transactions to the Joint Financial Intelligence Unit ("JFIU"); and
- assist the law enforcement authorities through providing an audit trail.

We do this through issuing guidelines that lay down the minimum standards that institutions should incorporate in their anti-money laundering systems. We then carry out on-site examinations to check that these standards are being adhered to. This year we introduced a two-tier, risk-based approach towards examinations. In cases where AIs may be at higher risk of money laundering, we conduct more in-depth examinations using specialist teams. This may involve sample testing and visits to branches to look at how controls actually work in practice and to ascertain at first hand the knowledge and awareness of staff. In more routine cases, higher level review of anti-money laundering controls is conducted, generally as part of our normal risk-based examinations.

We intend to supplement our own examinations with a system of self-assessment by compliance officers of AIs on risk indicators of money laundering within their own institutions and the quality of

controls. This will be done using a structured self-assessment framework that we aim to release to the industry later this year. This should help the HKMA to conserve its own resources and direct them where they are most needed. But it should also serve to remind AIs that they have the primary responsibility for making sure that their own house is in order.

The HKMA guideline

Checking that standards are being observed is obviously important. But it is necessary to ensure that the standards themselves remain effective in dealing with risks. That is why we are currently engaged in reviewing our anti-money laundering guideline.

In doing so, we are making particular reference to two main sources. The first is the paper on Customer Due Diligence for Banks issued by the Basel Committee in October 2001. The other is the consultation paper released by the FATF in May of this year on its review of the FATF Forty Recommendations that set the international standards on anti-money laundering. I would strongly recommend that all AIs familiarise themselves with both documents. Comments on the FATF Consultation Paper are due by the end of this month.

The process of revising the FATF Recommendations will probably not be completed until some time next year. Final revisions to our own guideline will probably have to wait until then. In the meantime, however, we are reluctant simply to leave our existing guideline unchanged. There may be a number of areas where it is possible for it to be updated to reflect the current international consensus and to draw together pieces of guidance on particular issues that have appeared in circulars over the last few years. We are considering the best way to do this. One option is to issue a supplement to the existing guideline, pending the final revisions. Whatever we do will, as always, be the subject of consultation with the industry.

In some places the revised standards may have to be tighter and permit fewer exceptions than at present. But we will try wherever possible to be sympathetic to AIs' concerns on compliance costs.

Terrorist financing

The most obvious thing we need to do is to incorporate into our guideline specific recommendations relating to terrorist financing. In particular, we need to make AIs aware of their responsibilities under the United Nations (Anti-Terrorism Measures) Ordinance that was enacted in July of this year and will begin to come into operation in the near future. The New Ordinance is intended to meet Hong Kong's commitments under the FATF's eight Special Recommendations on Terrorist Financing. To that end, it criminalises the financing of terrorism and associated money laundering and provides for the freezing of terrorist-related funds. It also imposes an obligation on AIs and other persons to report knowledge or suspicion that funds are linked to terrorism.

We have already asked AIs to report to the JFIU suspicious transactions that may be related to terrorism. But the legal obligation to do so is now clear and unambiguous, as is the criminal offence of dealing in terrorist funds. AIs therefore need to ensure that they have the necessary measures in place to comply with the law.

This is not an easy task. It is accepted that terrorist financing is difficult to detect even when AIs are provided with lists of terrorist suspects. The FATF published in April of this year a document called Guidance for Financial Institutions in Detecting Terrorist Financing that I would recommend you to look at. Among other things, this provides advice on the characteristics of financial transactions that may arouse suspicion, particularly when one or more of the parties is known or suspected to be a terrorist or terrorist organisation.

Even if there is no evidence of a direct terrorist connection, a transaction should still be reported to the JFIU if it looks suspicious for other reasons. This obviously applies to remittances as well as the opening of an account. It may subsequently emerge that there is a terrorist link. Thus, success in the fight against terrorist financing depends in large measure on the overall quality of AIs' controls against money laundering - in particular, their ability to detect suspicious transactions.

The customer due diligence process

This in turn depends on an institution's knowledge of its customers and what is a normal pattern of account activity for a particular customer. It is crucial therefore for AIs' to have effective systems for customer due diligence. The main essentials are already there in the HKMA's guideline, which requires AIs to make reasonable efforts to determine the customer's true identity. But the process may need to be articulated more clearly so that AIs are in no doubt about what they should be doing.

The FATF's Consultation Paper is useful in spelling out the main elements of the due diligence process, namely:

- to identify the direct customer;
- to verify the customer's identity;
- to identify the person with beneficial ownership and control, who may be different from the direct customer;
- to verify the identity of the beneficial owner and/or the person on whose behalf a transaction is being conducted; and
- to conduct ongoing due diligence and scrutiny.

A number of features stand out from this. First, the process of know your customer is a two-stage process - identification and verification. Second, there is a clear obligation on institutions to look behind the corporate veil, nominee or trustee to the ultimate beneficial owner. If necessary, this means following the chain of ownership or control to the natural persons at the very end of the chain. There are obvious practical difficulties in this, which we can discuss with the industry. But the basic issue is whether it is safe for institutions to establish a banking relationship if they do not really know with whom they are dealing.

The third point to note is that the due diligence process does not apply simply at the time the relationship with the customer is entered into. It must be an ongoing process using detection and reporting mechanisms that can pick up large or unusual transactions. The compliance officer appointed to take overall charge of the institution's anti-money laundering efforts should play an active role in the monitoring process and should not simply be the passive recipient of ad hoc reports from front-line staff.

It also follows that AIs must not only know their customer but also know their customer's business and the source of funds flowing into the account in sufficient detail to establish a benchmark against which to judge unusual transactions. This information will need to be updated, where appropriate, over the life of the account.

High risk customers

There is a certain basic amount of checking that must be done for all customers. But some may pose a higher than average risk of money laundering to the institution and thus require enhanced due diligence. AIs should therefore adopt a risk-based approach, with policies and procedures for identifying higher risk customers. We shall try to offer AIs guidance on the type of risk factors that they should be looking out for. But basically these factors can be summed up in terms of: *who* the customer is; *what* he does; *where* he comes from and *where* he does business; and *how* the account is operated.

Judged against these benchmarks, possible examples of high-risk customers that AIs should be on the look-out for, include the following:

- *politically exposed persons* - these are individuals holding important public positions and those related to them. Banks that deal with corrupt PEPs expose themselves to risk of bad publicity, legal action and possible financial loss;
- *other types of private banking customer* - particularly from those jurisdictions where the risk of money laundering is severe or whose business makes them more susceptible to money laundering;
- *correspondent banks* - particularly those from NCCTs or other high-risk jurisdictions where there are doubts about compliance with FATF standards. Specifically, AIs should beware of

so-called “shell banks”, which operate without a physical presence in their place of incorporation; and

- *corporate vehicles of various types* - including offshore companies and trusts where the objective may be to disguise the beneficial ownership.

Business introduced by intermediaries

Even with a risk-based approach, the process of identification and verification is an onerous one. It is natural therefore that AIs may wish to rely on the due diligence procedures undertaken by intermediaries who introduce business to them. However, experience has shown that this can expose institutions to risk if the intermediaries do not do their job properly. In particular, in Hong Kong, there have been a number of cases where secretarial companies or company formation agents have opened bank accounts on behalf of shell companies without conducting proper verification of the underlying principals. There are cases of such companies being used as the vehicle for bogus investment schemes.

We wrote to the industry on this last year, and the basic message bears repeating. While it is permissible for AIs to rely on intermediaries to carry out checks on the identity of potential customers and the source of their funds, the ultimate responsibility still rests with AIs to know their customers and their customers’ business.

Intermediaries should therefore only be used if the AI is satisfied that they apply due diligence standards and procedures as rigorous as those of the AI itself and are “fit and proper”. It helps in this respect if the intermediary is itself regulated or is the member of a reputable professional body. The AI should monitor the track record of the intermediary and the performance of the accounts that it introduces. All relevant identification data used by the intermediary to verify the customer’s identity should be submitted for review by the AI. This latter requirement is not currently mandated for all intermediaries in our current guideline; and we will need to consider whether this exception is still appropriate.

A further issue relates to the treatment of client accounts opened by solicitors or accountants. At present, we allow such intermediaries to rely on professional secrecy codes as a reason for not disclosing the identity of the underlying principals. Non-disclosure may be acceptable in the case of pooled accounts where the funds held by the intermediary are co-mingled at the bank. But where the account is opened on behalf of a single client, the justification is much less clear. Again, this is an area where change may be required.

Existing customers

As I have already mentioned, it is likely that AIs will have to upgrade their due diligence procedures in some respects to comply with changing international standards. Obviously, these enhanced procedures would be applied to new banking relationships. But this begs the question about what should be done in relation to existing customers. To what extent should institutions go back and undertake renewed verification of the identity of existing customers?

Our current view is that we should not impose an across the board requirement in this respect, but it would certainly be sensible to review those existing customers who fall into higher risk categories. The six major banks in the UK have just announced that they will undertake a risk-based initiative of this type. I would encourage those AIs with a large customer base to do the same. Other triggers for review of existing records may arise when a customer undertakes a significant transaction and where there is a material change in account operation or customer documentation standards.

The way forward

These are some, but by no means all, of the current issues we are considering in the context of our revised guideline. We hope to have something ready for consultation with the industry later in the year. While this may impose new obligations on AIs, we will try to ensure that these are of a nature that well-managed institutions would adopt of their own accord. After all, in essence, they amount to no more than being sure that you really do know your customer.