Money Laundering, Regulatory Strategy and Internal Corporate Controls

BRENT FISSE*

1. *Introduction*

Internal corporate controls are essential to the prevention of money laundering and should not be neglected at the level of international initiatives. The challenge is to devise flexible and efficient legal or administrative methods of inducing effective internal controls, especially within financial institutions, and to provide useful models which can be adapted to suit the legal culture and financial system of each member country of the United Nations.

The 44 recommendations on money laundering agreed to by the member countries of the Financial Action Task Force (FATF) may be taken as a convenient starting point. These recommendations are not confined to broader issues of policy and international co-operation — they also address the need for internal corporate controls against money laundering.

A. *FATF Recommendations on Internal Corporate Controls*

The main FATF recommendations relating to internal controls are as follows:

> *Recommendation 12*
>
> Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by selfregulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).
>
> *Recommendation 13*
>
> Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction is conducted if there are any doubts as to whether these clients or customers are not acting on their own behalf, in particular, in the case of domiciliary companies (that is, institutions, corporations, foundations, trusts, etc, that do not conduct any commercial or manufacturing business or any other form of commercial operations in the country where their registered office is located).

---

* Professor of Law, University of Sydney. This paper was prepared for a UN conference on money laundering organised by ISPAC and held at Courmayeur in June 1994.

Recommendation 14

Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Financial institutions should keep records on customer identification (for example, copies or records of official identification documents like passwords, identity cards, driving licences or similar documents), account files and business correspondence for at least five years after the account is closed.

These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

Recommendation 15

Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

Recommendation 16

If financial institutions suspect that funds stem from a criminal activity, they should be permitted or required to report promptly their suspicions to the competent authorities. Accordingly, there should be legal provisions to protect financial institutions and their employees from criminal or civil liability for breach of any restrictions on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report in good faith, in disclosing suspected criminal activity to the competent authorities even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Recommendation 17

Financial institutions, their directors and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

Recommendation 18

In the case of a mandatory reporting system, or in the case of a voluntary reporting system where appropriate, financial institutions reporting their suspicions should comply with instructions from the competent authorities.

Recommendation 19

When a financial institution develops suspicions about operations of a customer, and, when no obligation of reporting these suspicions exists, makes no report to the competent authorities, it should deny assistance to this customer, sever relations with him and close his accounts.

Recommendation 20

Financial institutions should develop programs against money laundering. These programs should include, as a minimum:

(a) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;

(b) an ongoing employee training program;

(c) an audit function to test the system.

Recommendation 21

Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

Recommendation 22

Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply these recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the mother institution should be informed by the financial institutions that they cannot apply these recommendations.

Recommendation 24

Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.

Recommendation 26

The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should cooperate and lend expertise spontaneously or on requests with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.

B. Unresolved Issues of Implementation for Discussion

These FATF recommendations focus attention on the need for internal controls against money laundering. However, they raise rather than resolve several important and difficult issues of implementation. There are at least three fundamental issues which seem to warrant discussion:

- What design criteria are relevant when assessing the adequacy of internal compliance controls and what steps should be taken to help ensure that the relevant factors are legally recognised and applied in practice?
- To what extent should control measures aimed directly at particular money laundering practices be specified in legislation or left to self-regulatory internal controls?
- Who is to be held responsible for non-compliance with control standards and what mechanisms should be used to help ensure accountability?

2. Corporate Compliance Systems

The extent to which corporations comply or do not comply with legal standards or prohibitions is largely a function of the adequacy of their internal control systems. In *Where the*

Law Ends: The Social Control of Corporate Behaviour, published in 1975, Christopher Stone made the important point that preventing corporate wrongdoing depended on internal corporate controls and that effective legal measures needed to relate specifically to those controls rather than treating the corporation merely as a "black box". Numerous commentators have since explored that basic idea and today there is a rich and diverse literature on issues of corporate compliance. However, there are relatively few commentaries on corporate compliance in the context of money laundering. As a result, there is some danger of neglecting lessons which have emerged from other areas of corporate regulation. The aim of this section is to set out a framework for the development of corporate compliance systems and then to mention some of the steps that could usefully be taken to help ensure that the key factors are recognised in law and applied in practice.

A. A Design Framework for Compliance Systems

Much more is involved in designing corporate compliance programs than merely having a compliance policy, "know your client" (KYC) procedures, training routines or auditing controls. This can be seen by viewing compliance controls from the perspective of corporate risk management or liability control.

(i) Key elements of compliance from a corporate risk management perspective

The following framework is suggested by reported experience and empirical studies of corporate compliance in a variety of regulatory contexts:[1]

- clearly stated compliance policies which are backed and reinforced by top management;
- systematic identification and management of risks created by the company's operations;
- clear allocation of responsibility for compliance functions to specified personnel;
- readable compliance manuals setting out relevant standards (legal, corporate, and industry self-regulating (for example, the Basle Statement of Principles on Money Laundering)) and enforcement agency guidelines, together with operating procedures for particular units in the organisation;
- routine controls for monitoring and enforcing compliance together with safeguards for ensuring command of compliance problems by senior management;
- review of loan and other contractual documentation in order to optimise the degree of self-protection;

---

1 See American Bankers Association, *Currency Transaction Reporting* (1988); Bank of Boston Corporation, *Bank Secrecy Act: Overview* (1990); Braithwaite, J, *To Punish or Persuade: Enforcement of Coal Mine Safety* (1985); Braithwaite, J, "Taking Responsibility Seriously: Corporate Compliance Systems" (1985) in Fisse, B and French, P (eds) *Corrigible Corporations and Unruly Law*, ch 3; Fisse, B, and Braithwaite, J, *The Impact of Publicity on Corporate Offenders* (1983); Adams, W, "The Practical Impact of Criminal Money Laundering Laws on Financial Institutions" American Bar Association (1990) *White Collar Crime National Institute* at 599; Fisse, B, Fraser, D and Coss, G (eds), *The Money Trail* (1992), chs 16–19; Drage, J, "Countering Money Laundering: The Response of the Financial Sector" (1993) 1(2) *Hume Papers on Public Policy* 60.

- control of documentation, including standard contractual terms for protection where secured assets are subject to confiscation, and procedures for avoiding the creation or retention of unnecessarily damaging or incriminating documentation;
- investigative and reporting procedures structured so as to maximise the protection possible from legal professional privilege (where that privilege is available);
- action plans in the event of discovery of illegality and for resolution of complaints received from employees, clients, members of the public, or enforcement agencies;
- education and training of personnel;
- regular interaction with the enforcement agencies responsible for administering the relevant statutes,[2]
- liaison with insurers and promotion of favourable insurance track record.

The exact mix and emphasis depends on various factors, most notably organisational structure, the particular nature of the firms' financial operations and usual client base, quality and number of personnel, the ability of top management to instil a culture of compliance without laying down detailed rules, and the extent to which achieving compliance and liability control is seen as a line rather than a staff function.

The framework above reflects a liability control, or risk management, perspective. The old-fashioned view of compliance systems revolved around the provision of legal services, whether by way of advice on particular transactions, education of personnel as to legal requirements, or periodic review of contractual and other documentation. A different approach has emerged over the past two decades. According to this approach, the basis on which compliance programs should be built is not only provision of legal services but management of risk of exposure to liability and related losses. This approach transcends legal advice and legal auditing:

- liability control systems justify their existence not on the quality or intensity of legal or other input by staff experts but on the contribution made to the company's profitability and reputation;
- management attitudes tend to carry more weight than the views of discrete compliance staff or outside professional advisers;
- compliance depends greatly on the day-to-day accountability of line managers and supervisors for operations under their span of command;
- legal auditing requires that compliance be monitored and the monitoring function is best undertaken as a line as well as a staff responsibility;
- suspected non-compliance is more likely to be reported upwards in an organisation through managers and supervisors than via specialised legal staff;
- self-protective documentation programs require not only legal auditing but also procedures which are ingrained down the line;

---

2 See generally Sigler, J A and Murphy, J E, *Interactive Corporate Compliance: An Alternative to Regulatory Compulsion* (1988).

- responding to complaints from consumers, employees, or enforcement agencies is not only a defensive legal function but also a feedback mechanism for managerial learning;
- education and training are more obviously achievable through routine operational procedures than by reliance merely on periodic lectures and seminars conducted by compliance staff or solicitors from law firms.

B. Harmonising State Crime Control Strategies and Corporate Risk Management

The framework set out above relates to the position of organisations subject to money laundering controls by the state. By contrast, the approach taken in the FATF recommendations views corporate compliance from the angle of state crime control strategies. If the FATF recommendations or others to like effect are to take hold in practice, then state-oriented visions of social control need to be complemented by corporate-oriented assessments of the interests and motivations of the financial and other institutions whose support is sought in the fight against money laundering. Unless this is done, conflicts and disharmonies can and will arise between state-oriented control measures and corporate measures of liability control.

Disharmony between state crime control and corporate risk management surfaces where financial institutions are put at risk of committing money laundering offences if, as a result of trying to comply with money laundering control obligations, they are also likely to engage in conduct which amounts in law to an offence. The Australian *Financial Transaction Reports Act* (1988) and related money laundering statutes illustrate this problem.

(i) Illustrative Australian legislative disharmonies

- The "no-knowledge" provision under section 17 of the *Financial Transaction Reports Act* immunises the information contained in a suspect transaction report and not other incriminating evidence of which the defendant may quite reasonably be aware. Under section 17, a cash dealer, or an officer, employee or agent of a cash dealer, who provides information in a suspect transaction report or otherwise under section 16 is deemed not to have been in possession of that information for the purposes of the money laundering offences under sections 81 and 82 of the *Proceeds of Crime Act* 1987 (Cth). The wording of this immunity is too narrow. The information communicated under section 16 is a re-statement, usually in summary form, of the information in the possession of the cash dealer or one or more of its representatives. The information that must be reported under section 16 by no means exhausts all the details that may be known to a cash dealer or its employees. The immunity under section 17 extends only to "that information", that is the particular information communicated under section 16(1) or (4). It does not cover other information which is not communicated under section 16 but which, independently of the details communicated in compliance with section 16, may amount to knowledge or reason to know or suspect the tainted nature of a transaction required for the mental element of the offence of money laundering. If so, the cash dealer or employee has acted with the mental element required for the offence of money laundering under either section 81 of the *Proceeds of Crime Act* (which requires knowledge or reason to know) or section 82 (which requires a reason to suspect), and could be held criminally liable under those provisions. In other words, cash dealers or their employees who act in good faith and who have taken all necessary steps to comply with section 16 are not adequately

protected against liability for money laundering contrary to section 81 or section 82. The undue narrowness of the immunity under section 17 could and should be overcome by amending the section. The amendment should expressly provide that there is no liability under section 81 or section 82 where the communication of information under section 16 is sufficient to convey, in summary or detailed form, the centrally material facts which suggested or indicated to the cash dealer or its representative that the money or other property involved in the particular transaction reported was derived or realised, directly or indirectly, from some form of unlawful activity.

- The structured transaction or "smurfing" offence under section 31 of the *Financial Transaction Reports Act* does not contain a safe harbour provision for financial institutions or their employees in cases where cash transactions are entered into in order to discover the identity of those engaged in the unlawful structuring of transactions. The thrust of the *Financial Transaction Reports Act* is to encourage financial institutions to assist the detection of money launderers and indeed their assistance in the difficult task of uncovering smurfing operations and the ringleaders behind them is vital. Detection is unlikely to be possible unless deposits are accepted and then checked. However, by accepting a deposit, a finance company or bank then becomes a party to a transaction which may expose it to criminal liability under section 31. Immunity against liability under section 31 cannot be achieved by making a suspect transaction report under section 16. Action taken pursuant to section 16 (making a suspect transaction report or giving further information required under section 16(4)) is immunised under section 16(5). However, being a party to a structured transaction as defined in section 31 is not action taken pursuant to section 16. Nor is there any protection under the "no knowledge" rule in section 17: the immunity under section 17 is confined to money laundering offences under section 81 and section 82 of the *Proceeds of Crime Act* (Cth). A cash dealer and its employees are thereby placed in an invidious and unacceptable position. To make a suspect transaction report is to provide incriminating evidence of one's involvement in a structured transaction and thereby to run the risk of liability under section 31. Not to make a suspect transaction report is to violate section 16 and, quite possibly, to spark a prosecution for money laundering under section 81 or section 82 of the *Proceeds of Crime Act* (Cth). The solution required is a safe harbour provision which exempts parties from liability under section 31 if a suspect transaction report is filed in relation to the transaction in accordance with section 16.
- Where a suspect transaction report is made under section 16 in relation to a transaction it will be virtually impossible later in the context of forfeiture proceedings to exclude an interest of the bank or finance company created by the transaction. By hypothesis, the bank or finance company will have had a reason to suspect the transaction and if the bank or finance company proceeds with the transaction that it has reported as suspect it runs the risk that an interest created by the transaction will be subject to a restraining order and eventually to forfeiture as well. The immunity provisions under section 16(5) and section 17 of the *Financial Transaction Reports Act* do not apply to this situation. This is highly unsatisfactory, and section 16(5) requires amendment to provide a safe harbour for financial institutions in such a position.

(ii) Legal exemptions or administrative "assurances"?

It is sometimes claimed that financial institutions and their employees have nothing to fear in situations of the kind discussed above because they will never be prosecuted if they acted in good faith. Such a posture hardly confers a legally effective immunity. One danger is that the facts of the case where a financial institution happens to be prosecuted may differ from those contemplated by the representative of the enforcement agency when attempting to give that "assurance". Another danger is that the enforcement agency may change its policy or practice from time to time. Why not give stable and legally effective guarantees of non-exposure to criminal liability through a clear and adequate statutory definition of the conduct prohibited?

(iii) Excessively limited focus of FATF Recommendation 16

FATF Recommendation 16 provides that those who, in good faith, report their suspicions about money laundering to the authorities should be protected against criminal or civil liability "for breach of any restrictions on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision".

The safe harbour proposed in Recommendation 16 is commendable but does not go far enough to avoid the conflict and disharmony discussed above. The problem is broader than that posed by laws relating to privacy or confidentiality and exists in any situation where state control measures require action to be taken by a financial institution but where compliance with that obligation is likely to expose the institution to criminal liability, liability to civil penalties or forfeiture of a legitimate interest in tainted property.

C. Embedding Compliance Precepts

If it is agreed that compliance with international money laundering control standards does depend heavily on whether those standards can be translated into effective compliance controls within financial institutions and other organisations, then what can be done at the international level to assist that process?

Several initiatives within member countries of the United Nations could be encouraged and the lessons flowing from the pursuit of compliance within organisations could be collected and made available for ready distribution:

- National money laundering control statutes could spell out both the need for financial institutions to have responsive internal control systems in place and the importance attached to that objective.
- A design framework for compliance systems could be set out in regulations or in an explanatory memorandum accompanying the relevant local money laundering legislation.
- Details of the content of compliance systems adopted by a representative range of financial institutions, together with case studies of compliance initiatives in a variety of firms, could be compiled by enforcement agencies together with recommendations about the features considered to be the most conducive to effective compliance. Comparative descriptions and analyses of compliance systems used by financial institutions in different countries could also be developed under the auspices of, for example, ISPAC.
- Enforcement agencies could be expressly encouraged to stress compliance systems in their surveillance and negotiations with financial institutions and to include specific compliance-related provisions in the terms of settlements entered into with those institutions as a result of enforcement action. Details of such settlements could be filed with and distributed through an international clearing-house.

- The legal framework for dealing with institutions found to have been implicated in unlawful money laundering activities could be geared so as to focus more on internal controls and the need for revision and/or supervision. Corporate probation is one mechanism suitable for this purpose; the statutory injunction is another. The empowering provisions could expressly authorise the use of probation and injunctions as a means of spurring better internal controls and achieving their implementation.
- Self-regulatory initiatives in relation to the design of effective compliance programs could be further encouraged within the banking and finance industry and fostered by means of a compliance clearing-house so that the fruits of such activity in one country could readily be shared with enforcement agencies and financial institutions in other member countries of the UN.

In short, the policies expressed in the FATF Recommendations raise practical questions of implementation at the micro-level of the organisations where money laundering activities take place around the world. At that level, the concerns and the experience are specific and localised but, just as an international and comparative analysis of the behaviour of firms is widely thought to be essential in the context of economics, an international and comparative analysis of the conduct and compliance methods of firms seems essential in the context of money laundering.

3. *Controls Aimed Directly at Money Laundering Practices — Enforced Self-Regulation and Technological Change*

As evidenced by the FATF Recommendations, money laundering control measures require that financial institutions take steps (for example, reporting suspect transactions) to block money laundering. An important question of regulatory design is the extent to which the standards imposed under such control measures should be prescribed in detail in the scheme of regulation or left more to the institution to work out as a matter of self-regulation. The FATF Recommendations understandably give each member country considerable leeway to devise an approach consistent with its own regulatory culture. The discussion below outlines some of the directions which are open and which seem worth further consideration.

A. Enforced Self-Regulation

The enforced self-regulation model advanced by John Braithwaite[3] is one interesting possible direction to be considered. This model, which is of general potential application, has recently been extended by Braithwaite to the field of money laundering.[4]

The first postulate of the model is that financial institutions differ widely, so widely that universalistic command and control prescriptions are bound to be inefficient for many organisations:[5]

---

3 Braithwaite, J, "Enforced Self-Regulation: A New Strategy for Corporate Crime Control" (1982) 80 *Mich LR* 1466.

4 Braithwaite, J, "Following the Money Trail to What Destination?" (1993) 44 *Alabama LR* 657.

5 Id at 664.

> All banks are different. They deal with different sorts of clients. They have different histories of how they have successfully solved their problems and what has failed to work for them in the past. In addition, they have disparate corporate cultures. Consequently, a strategy for detecting money launderers that works well in Bank A may fail in Bank B; a strategy that has a low cost for A may have a high cost for B. The problem with government command and control regulation is its commitment to the public law principle of consistency; it would be unjust to regulate A more aggressively than B unless A has engaged in conduct that makes it deserving of extra intervention. Therefore, the same regulatory requirements are imposed on Banks A and B, irrespective of their likely effectiveness and costs in the context of those organizations.

A second postulate is that it is possible to avoid going to the opposite extreme of self-regulation. Financial institutions can be given the same performance objectives and required to have their own particularistic plan for achieving those objectives efficiently:[6]

> Once the bank has come up with a money laundering control plan that satisfies the government that it is likely to meet its objectives or standards, the state motivates the bank to enforce its plan through the threat of enforcement action against the bank for failure to do so. The idea, therefore, is privately written and publicly ratified rules. These rules are then primarily privately enforced, with secondary public enforcement where private enforcement fails. It is thus an attempt to improve on the inflexibilities and costs of command and control regulation while responding to the naivety of trusting business to regulate itself.

The enforced self-regulation model holds much appeal in the abstract but in practice it can be difficult to work out exactly how far it should be taken or indeed whether it is a practical option. Some of the more difficult issues posed by the model in the context of money laundering are canvassed below.

B. Suspect Transaction Reporting

The model of enforced self-regulation envisaged by Braithwaite for suspect transaction reporting envisages that financial institutions would be required to spell out the particular way in which they would go about detecting suspect transactions and ensuring that staff acted according to that plan:[7]

> This enables the bank to design rules that are in tune with what works within their corporate culture and that will impose minimum costs given the way they are set up to do business. Trust-based corporate cultures may rely more on work groups meeting together to share "know your customer" suspicions and leads that might detect the laundering of proceeds of crime. Conversely, rulebased corporate cultures with a strong educative emphasis may rely on very detailed rules for reporting specified types of transactions where those rules are the subject of elaborate corporate training programs. Rule-based corporate cultures with a strong disciplinary emphasis may rely less on in-service training than on a corporate track record for immediately firing employees who have failed to teach themselves the rules and to implement them.

This approach is seen as more conducive to the protection of privacy as well as more efficient in terms of corporate impact:[8]

---

6 Ibid.
7 Id at 665.
8 Id at 666.

> Tailor-made money laundering detection plans might not only be less costly and more effective in terms of the detection of money launderers, but also more effective in preventing unnecessary invasions of privacy. Instead of reporting all suspicious transactions to the state so that huge numbers of citizens have their affairs listed on criminal intelligence data bases for quite insufficient reasons, banks can design their own procedures for internal investigations of suspicious transactions in their money laundering prevention plans. These procedures would be approved by the state, thereby limiting the number of reportable cases to those which continue to be suspicious after the agreed upon in-house tests have been applied. More citizens could have knowledge of their financial affairs confined within the walls of the banks to which they entrusted that knowledge.

Enforced self-regulation would not preclude small institutions from developing their own tailor-made systems: a "money laundering control systems consulting industry" could be expected to emerge. Consultants would supply "a variety of off-the-shelf control systems, the choice from competing systems being guided by the size, history, customer base, and corporate culture of the particular bank."[9]

Braithwaite contends that there would be innovation, not only in the software of detection diagnostics and in "know your customer" information processing, but in performance evaluation as well:[10]

> Banks could be required to undertake triennial reviews of how many true and false money launderers they had detected as part of their approved control plan. Moreover, the reviews could diagnose the aspects of their plans that were responsible for the true positives versus the false positives as well as the characteristics of false negatives — customers who were detected to be money launderers by some means other than the money laundering control plan. Performance indicators for such evaluations could relate not only to detection, but also to cost and privacy protection indicators. Indeed, true positive/false positive ratios might be designed to incorporate all three of these performance criteria.

The approach suggested is a welcome contrast to the orthodox and rarely tested assumption that suspect transaction reporting is in fact effective and worth the cost it imposes on financial institutions and the law enforcement agencies who subsequently follow up on the reports. However, it is doubtful whether enforced self-regulation should extend that far.

One feature of Braithwaite's suggestion is that the onus and expense of the research and development is cast on to organisations without any apparent prospect of recoupment apart from the possible savings made by reduced exposure to loss through money laundering. Not all will agree with that position. It is unclear why the social cost of improving suspect transaction controls against money laundering should be imposed mainly on financial institutions rather than spread more through general taxes in the same way as many countries spread the costs of improving stolen vehicle tracking systems or enhancing surveillance technology for detecting terrorists or plane hijackers.

A more fundamental question, and one suggested by Braithwaite's plea for empirical testing, is whether suspect transaction reporting should be given the major role it is supposed to play in jurisdictions where this control measure has been adopted. First, it is difficult to distinguish between objectively suspect transactions and those which, short of the threshold, are merely suspected. Secondly, the suspect transaction test is narrower than that of

---

9 Ibid.

10 Id at 667.

"unusual" transactions and may easily exclude highly useful intelligence. Unusual transactions may provide critical investigative linkages, which partly explains why FATF Recommendation 15 envisages that financial institutions will keep a watch out for "unusual" patterns of transactions. Thirdly, the recent UK study by Michael Levi[11] indicated a very low strike-rate — around one *arrest* of a suspected drug trafficker per 200 suspect transaction reports. Fourthly, the sheer number of transactions handled by most financial institutions means that any checking of particular transactions is likely to be cursory and quite possibly unreliable.

These concerns have led Levi to suggest that the emphasis should not be on suspect transaction reporting but on the use of knowledge based systems, neural networks and artificial intelligence means of detecting potential cases of money laundering. If that direction be taken, then one implication is that financial institutions will not be required to devise their own detection and self-evaluative programs but will instead be obliged to provide data in standard formats so that the intelligence can readily be captured and analysed by a central enforcement agency. This move away from suspect transaction reporting and towards cyberwatch systems is perhaps inevitable — the more automated the banking and financial system becomes, the less face-to-face contact between clients and employees and the greater the holes in the detection net unless client information is electronically scanned for abnormal patterns and connections. This growing reality has been recognised in Australia in the context of significant cash transactions reports and details of all wire transfers — the data is automatically sent by the banks to the Australian Transaction Reports and Analysis Centre (AUSTRAC) for checking and the checking process involves a variety of pattern matching and other computer-based detection routines.[12]

C. Anti-Smurfing Deposit Aggregation Requirements

Internal controls by financial institutions against structured transactions (smurfing) work on the basis of checks for cash deposits by a customer which in aggregate exceed the threshold amount at which a single cash transaction must be reported. One major difficulty is to indicate to financial institutions the time-frame within which they are obliged to aggregate cash deposits without also letting smurfs know what adjustments they need to make to avoid getting caught by the aggregation tests. This problem, which haunts any cash transaction reporting system, is illustrated by the Australian anti-smurfing provisions.

The smurfing offences under section 31 of the *Financial Transaction Reports Act* 1988 (Cth) are defined essentially in terms of the test whether, given the nature of the transactions, it is "reasonable to conclude" that a dominant purpose of the transactions was to evade the reporting obligations under the Act. The test under section 31 is not related to any given period during which financial institutions are expected to aggregate transactions involving a particular customer. There is no specific obligation under the Act to aggregate deposits or other cash transactions. Instead, "the aggregated value of transactions" is one of the indicia (see section 31(1)(b)(i)(B)) which the trier of fact is to consider when applying the "reasonable to conclude" test.

The ex post facto nature of the test of liability under section 31 puts banks and other financial institutions in a precarious or impossible position. The "reasonable to conclude"

---

11 *The Reporting of Suspicious Money Laundering Transactions* (1994).

12 See AUSTRAC, *AUSTRAC Papers 1992*. AUSTRAC operations are reviewed in Australia, Senate Standing Committee on Legal and Constitutional Affairs, *Checking the Cash* (1993).

test implies that financial institutions are under an obligation to aggregate cash transactions yet they are not in a position to know what that obligation requires of them at the time when the transactions take place. Worse, the test is not applied until the matter is determined by the trier of fact. Financial institutions thus remain under an obligation to aggregate until such time as the matter is decided in a prosecution or civil proceeding. So open-ended an obligation to aggregate is not merely vaguely defined but quite impractical. To comply with it, conceivably a bank would need to aggregate deposits on a perpetually rolling basis, perhaps for years after an initial transaction took place. If the legislation does not require banks to go to such extreme lengths, where is the line to be drawn?

It is also unclear whether the required standard of compliance is the same across the wide variety of organisations and bodies subject to section 31, or whether it varies depending on the technology available to the particular organisation. What exactly are banks and other cash dealers supposed to do to keep track of deposits or other transactions at their various branches? A major interstate or international bank may have a sophisticated computer network which makes the task of aggregation a relatively simple one, whereas a small finance company may lack any corresponding facility. If, for example, a bank has a computer-based tracking capability that enables it instantaneously to aggregate all deposits made at any branch within, say, a 24 hour period, then it may well be "reasonable to conclude" on the basis of the information available to that bank that the sole or dominant purpose of the customer was to evade the reporting requirements. On the other hand, if a bank does not have such a computer-based capacity, perhaps it is unreasonable to arrive at the same conclusion. Section 31 does not resolve the most critical question here, which is whether or not banks are expected to install systems that will enable aggregation of deposits made at all branches, instantaneously or within say a daily or other period. Many financial institutions in Australia as elsewhere do not presently have the capacity to aggregate deposits at all branches even on a daily basis. If they are expected to acquire some greater capacity, it seems harsh to make them run the gauntlet of an ill-defined penal provision. Moreover, installing adequate systems takes time and systems cannot sensibly be installed until it is known what exactly the expected standards of aggregation are.

One possible solution would be a system, developed in conjunction with the banking and finance industry, under which different aggregation periods are used by different financial institutions at different periods arranged on a secret roster basis.[13] Financial institutions would then know exactly where they stand, yet smurfs would not be presented with aggregation rules which could easily be circumvented. Such a system supposes that banks and other financial institutions have the technical capability to alter the time settings of their aggregation programs periodically at low cost. It also assumes that the roster arrangements could in fact be kept secret from the smurfing underworld.

Another possible approach is via enforced self-regulation, with each bank determining its own aggregation rules — smurfs would not be faced with a standard aggregation period which could easily be circumvented but with many unknown and different aggregation periods.[14] This approach assumes that the aggregation period selected by a given bank could in fact be kept secret from smurfs. It does not necessarily assume a technological capacity to change the aggregation periods periodically at low cost. However, such a capacity might well be essential to reduce the risk of disclosure.

---

13 See Fisse, Fraser and Coss, above n1 at 186.

14 Above n4 at 665.

The only approach capable of avoiding the otherwise high risk of the aggregation periods being leaked to smurfs is a centrally controlled system under which aggregation periods for each and every financial institution are selected randomly by a computer program in such a way that no human agent has access to the random sequence. As in the case of suspect transaction reporting, the solution which may ultimately be arrived at could well be driven much more by technology and software innovation than by the regulation versus self-regulation debate.

4. *Accountability for Non-Compliance with Money Laundering Controls*

As international initiatives against money laundering increasingly move beyond the macro-level and focus more on the operational or micro-level of securing compliance by financial institutions and the commercial sector generally, an important question is how accountability is to be imposed in the event of non-compliance. FATF Recommendation 7 exhorts member countries to rely on corporate criminal responsibility as well as individual criminal responsibility and Recommendation 8 urges that consideration be given to using a variety of sanctions including civil penalties. Even with such tools available, however, it is often difficult to impose accountability for non-compliance, especially in a context like money laundering where the main participants are typically large organisations. This problem invites further consideration because, unless it is resolved in a practical way, efforts to control money laundering may easily break down.

Two major problems of accountability for corporate crime are typical in modern societies:[15]

- There is an undermining of individual accountability at the level of public enforcement measures, with corporations rather than individual personnel frequently being made the prime target of prosecution. Given the practical difficulties of unravelling individual accountability within organisations, enforcement agencies and prosecutors are inclined to take the short-cut of proceeding against corporations rather than against their more elusive personnel. Individual accountability thus tends to be displaced by corporate liability, which serves as a rough-and-ready catch-all device.
- Where corporations are sanctioned for offences, in theory they are supposed to react by using their internal disciplinary systems to sheet home individual accountability, but little or no attempt is made to ensure that such a reaction occurs. The impact of enforcement can easily stop with a corporate pay-out of a fine or monetary penalty, not because of any socially justified departure from the value of individual accountability, but rather because that is the cheapest or most self-protective course for a corporate defendant to adopt.

These problems are far from trivial. Individual accountability has long been regarded as indispensable to social control, at least in Western societies. The danger of "headlessness" has often been stressed, as by John Stuart Mill in *Considerations on Representative Government*:[16]

---

15 See further Fisse, B and Braithwaite, J, *Corporations, Crime and Accountability* (1993).

16 Gray, J (ed), *John Stuart Mill: On Liberty and Other Essays* (1991) at 393.

> As a general rule, every executive function, whether superior or subordinate, should be the appointed duty of some given individual. It should be apparent to all the world who did everything, and through whose default anything was left undone. Responsibility is null when nobody knows who is responsible.

Introducing corporate criminal responsibility, as envisaged by FATF Recommendation 7, hardly goes far enough. The prime issue is not whether corporations can be held responsible but whether it is possible to secure an effective mix of individual and corporate responsibility.

Likewise, civil penalties do not resolve the basic issue of accountability. Useful as it may be to have this option available as well as criminal prosecutions and civil remedies, difficulties still stand in the way of upholding individual accountability and achieving a workable and effective balance between individual and corporate liability for penalties.

Nor is forfeiture well-suited to the challenge of securing accountability. The sanction of forfeiture is largely monetary in effect and, where imposed on financial institutions, the impact is likely to be borne by shareholders rather than by the managers responsible.

A. Extending Accountability via Corporate Discipline and Disclosure

If accountability for money laundering is to be taken seriously, one starting point is the following rule of action:

> [S]eek to publicly identify all who are responsible and hold them responsible, whether the responsible actors are individuals, corporations, corporate subunits, gatekeepers, industry associations or regulatory agencies.

This rule of action could conceivably be implemented under an enforcement strategy which, in addition to relying on criminal or other public enforcement actions against individual suspects, harnesses the private justice and internal control capacities of organisations. The central idea is that corporate liability be used as a lever for achieving individual accountability at the level of internal corporate discipline or disclosure. As the Law Reform Commission of Canada has pointed out, corporate liability is potentially an efficient dispenser of individual accountability:[17]

> In a society moving increasingly toward group action it may become impractical, in terms of allocation of resources, to deal with systems through their components. In many cases it would appear more sensible to transfer to the corporation the responsibility of policing itself, forcing it to take steps to ensure that the harm does not materialize through the conduct of people within the organization. Rather than having the state monitor the activities of each person within the corporation, which is costly and raises practical enforcement difficulties, it may be more efficient to force the corporation to do this, especially if sanctions imposed on the corporation can be translated into effective action at the individual level.

The aim is thus to find a way of imposing individual accountability across a far broader range of cases than is feasible given the limited resources of state enforcement agencies. The sanctions available through private justice systems (for example, dismissals, demotions, shame, exposure) may be less potent than gaol or community service, but there is nonetheless a case for imposing weaker sanctions on many personnel rather than resorting to stronger sanctions against very few as is now common.

---

17 Canada, Law Reform Commission, *Working Paper 16, Criminal Responsibility for Group Action* (1976) at 31.

There are various possible ways in which such an approach could be implemented. For example, where the conduct elements of an offence are proven to have been committed by or on behalf of a corporation, the court, if equipped with a suitable statutory injunctive power, could require the company (1) to conduct an enquiry as to who was responsible within the organisation and outside it, (2) to pin-point those responsible and to take disciplinary action against all responsible parties over whom the organisation had such power, and (3) to return a report detailing the lines of responsibility and the action taken. If the corporate defendant returned a report demonstrating compliance with the above requirements then corporate criminal liability would not be imposed. If the company inexcusably failed to comply then both the company and its top managers[18] would be criminally liable for their failure to comply with the order of the court; the range of sentences for corporate defendants might well include probation, court-ordered adverse publicity, and community service. The same approach could also be implemented by means of undertakings or consent agreements entered into as a result of enforcement negotiations and settlements.

More concretely, it is instructive to consider what might have been done in the case of the Bank of Credit and Commerce International Ltd (BCCI) to achieve accountability under such an approach.

B. BCCI and Accountability[19]

The systematic culture of money laundering at the highest levels within BCCI and the consequential issue of accountability has not been addressed adequately by the few prosecutions which have occurred.

A more effective approach at the time of the first prosecutions would have been to hold BCCI civilly liable for having engaged in money laundering and to proceed on that platform to uncover the responsibility of those implicated in the web of illegality. Top management of BCCI would have then been brought in and required by the court to complete a full internal investigation of money laundering in all the bank's international operations, not just those in the country of the detected offence. Preferably, this would have been conducted with the assistance of an *independent* outside accounting firm.[20] More critically, the court would have required specified top management officials to certify (under threat of imprisonment for contempt) that the bank had disclosed all of its international money laundering activities. Perhaps the top management team might then have refused to cooperate:[21] the extent and seriousness of BCCI's money laundering was so breathtaking that no top management officer might have been prepared to put their neck in this disclosure noose; alternatively, a tactical decision might have been made to resist disclosure on the

---

18 As a condition of an injunction or a compliance agreement, particular managers (including senior managers) could well be assigned primary responsibility for ensuring compliance; see Geraghty, J A, "Structural Crime and Institutional Rehabilitation: A New Approach to Corporate Sentencing" (1979) 89 *Yale LJ* 353 at 372; Canada, Law Reform Commission, *Working Paper 16, Criminal Responsibility for Group Action* (1976) at 35.

19 The account below is adapted from Fisse and Braithwaite, above n15 at 222–7.

20 In fact, the Bank of England subsequently did require Price Waterhouse to conduct an "independent" investigation. But Price Waterhouse was far from independent. It was BCCI's sole auditor since 1987: *Australian Financial Review*, 17 Sept 1991 at 14; see also *Financial Times*, 15 May, 1992 at 7; 12 March, 1992, at 8.

21 In fact, however, what BCCI top management did was to cooperate with the investigations that did occur, while using a variety of stalling tactics.

basis that the court lacked jurisdiction to obtain details relating to the bank's operations abroad. Such a response would have sounded alarm bells.

A full-scale investigation would have then swung into action. This inevitably would have turned up insiders who were willing to reveal the complex story of the illegal bank within a bank (as they subsequently did when the Bank of England and the US Congress finally conducted a wider-ranging investigation in 1991). As soon as the wider investigation showed that the reason for the refusal to cooperate with a self-investigation report was the enormity of the top management fraud, one of the governments concerned could then have gone over top management's head to the shareholders — the ruler and government of Abu Dhabi. This would have been followed by inexorable political pressure for government to government demands for cooperation, with full disclosure of the malfeasance of the bank.

Whether by voluntary disclosure, by government investigation or by inter-governmentally forced disclosure, the court would have produced a document revealing that there was a secret bank within a bank at BCCI that engaged in massive fraud itself and that moved money for other major international fraudsters, for the very biggest drug empires, for terrorist groups, for Manuel Noriega and Saddam Hussein, for covert nuclear programs, and for illegal arms sales to Iran.[22] The court would have learned that by 1988 the then CIA director's nickname for the bank — the "Bank of Crooks and Criminals International" — had wide currency. It would have become clear to the court that a possible reason for this extraordinary nest of international criminality was that the bank was set up in such a way that it had no home regulator. It was effectively offshore in every country in which it operated. In response, the court could have opened up a more searching enquiry, conducted by honest elements within the bank working with outside consultants, to reveal to the public the full story of the regulatory failures that had occurred. What were the loopholes in the 1983 Basle Concordat on shared international regulation of banks that allowed BCCI to be effectively offshore everywhere?[23] Why did BCCI provide free travel to the Secretary-General of the United Nations, to Jimmy Carter, and more extravagant benefits to many other prominent international political figures?[24] How should the international banking system and the international banking regulatory system be reformed to prevent latter-day BCCIs from springing up?

If responsibility for corporate money laundering is to be imposed at all effectively, the courts need to impel the publication of accountability reports which document the responsibility of all who are responsible and which examine or at least draw attention to the institutional responses likely to be necessary to thwart repetition of offences. In a case like that of BCCI, where the Governor of the Bank of England was among those partly responsible,[25] the court would have a role that can stand independently above the failings of the international club of regulators. Some regulators have claimed that they had to hold back

---

22 In 1986, the CIA advised several other US government agencies that BCCI was a criminal organisation (*Financial Times*, 2 August, 1991 at 6). When Benazir Bhutto became Prime Minister of Pakistan in 1988, she was so advised by "friends in America" (*Wall Street Journal*, 5 August, 1991 at A11).

23 *Financial Times*, 22 July, 1991 at 12. The Basle Concordat has now been amended with a view to having large international banks regulated on a worldwide basis by a single bank regulator (*Financial Times*, 7 July, 1992 at 3).

24 *Financial Times*, 27–28 July, 1991 at 4; Kerry Report, *The BCCI Affair* (1992) at 11.

25 See "Senate Accuses Bank and Government over BCCI" *Guardian Weekly*, 11 Oct, 1992 at 18.

in order to prevent a run that would harm depositors. Critics have responded that their inaction brought more innocent victims into the web and that "the Bank [of England] might have been more concerned about Middle East relations than protecting depositors".[26] Stronger critics allege that the key players in the central banks or finance ministries of a dozen nations took bribes from BCCI.[27]

Faced with cases of the enormity of BCCI, the criminological tradition has been to evince a policy analysis of despair. Nikos Passas has provided an incisive analysis of the reasons for pessimism about controlling such corporate crime.[28] Passas identified four particularly intransigent difficulties in the BCCI case:

1. *Inter-Agency Conflicts, Miscommunications and Inertia.* The most critical failure here was that the CIA's 1986 report on the criminality of BCCI was distributed to some but not all federal enforcement agencies (critically, not to the FBI and the DEA). Investigations were compartmentalised in a way that missed the big picture of systemic criminality. So the Bank of England was naively allowed to believe that BCCI had a few rotten apples that were being removed from the barrel.
2. *Inadequate Resources.* An integrated investigation would have been impossibly costly for most enforcement agencies in most countries.
3. *BCCI's Power.* Partly this was the power of cultivating some of the most influential political figures in the world. But it was also the power of harbouring the secrets of the CIA, British, French, and Swiss intelligence and other such clients who had used the services of the bank. There was also the power of the major shareholders, the Sheik of Abu-Dhabi and his government. Ultimately, the most persuasive power was the fear of disrupting Western Arab relations and even of touching the White House through opening up the bank's role in the Iran-Contra affair.
4. *Legal Restraints.* Secrecy provisions in many national banking and tax laws and the difficulties of extraterritorial enforcement were an effective last line of defence for the bank.

There is no simple panacea to these massive difficulties, but they can and should be tackled.

- Points 1 and 2 above can be tackled by motivating the defendant corporation to pay for independent counsel to pull together all the threads of the entire tapestry of responsibility. In the BCCI case, the desire to prevent a sudden collapse of all the bank's operations or withdrawal of all the bank's operating licences as a result of court-ordered publicity might have been a potent motivation.
- Point 3 can be tackled by separating the powers of courts from those of the state in a functioning democracy: an independent judge has less reason to worry about what the

---

26 *Financial Times*, 12 March, 1992 at 8.

27 Truel, P and Gurwin, L, *False Profits: The Inside Story of BCCI, the World's Most Corrupt Financial Empire* (1992) at 168.

28 Passas, N, *Regulatory Anaesthesia or the Limits of the Criminal Law? The Prosecution of BCCI for Money Laundering in Tampa, Florida* (1993).

White House, John Major, the CIA or the Bank of England thinks than does the head of a US government agency.

- Point 4 can be tackled by not relying directly on national laws to empower investigators; it is possible to rely on the self-investigative and internal disciplinary capacities of the defendant corporation. These capacities are no more limited by the sovereignty of national law than is the corporation's capacity to commit transnational crime. If the corporation has the will to find out what happened through its international transactions, it generally has the capacity to do so.

A core problem apparent from the BCCI case is that accountability for corporate crime has yet to be conceived and structured in such a way as to encourage courts to pursue the issue of allocation of responsibility in complex cases and to achieve the wide measure of disclosure and accountability that is often required. Unless efforts towards reconceiving and restructuring the role of courts in this area are made, it is difficult to see how, as a practical matter, the international control strategies which are being developed against money laundering can be enforced in the worst corporate cases of non-compliance where effective enforcement is most needed.

Upholding accountability is hardly the only major problem which arises in controlling international money laundering where financial institutions are implicated. The limited point raised here is that it is one major issue which has yet to be resolved.

5. *Conclusion: Controlling Corporate Money Laundering*

Internal corporate controls are essential to the implementation of any legislative or regulatory program aimed at money laundering and warrant further consideration at the level of international initiatives against money laundering. Although it is tempting to focus on more overarching issues of international enforcement, the view expressed in this paper is that effective strategies for controlling money laundering require attention to all major problems of implementation including the difficulties of achieving compliance within financial institutions.

This paper has set out the following items for further consideration and debate:

- a framework for assessing the adequacy of internal corporate compliance controls and suggestions for promoting the legal recognition and application of key compliance precepts;
- a perspective on the regulation v self-regulation debate through the prisms of enforced self-regulation and technological change, with particular reference to suspect transaction reporting, and aggregation of deposits for the purpose of countering smurfing;
- a review of the importance of accountability for corporate non-compliance with money laundering control standards, together with suggestions as to how accountability for corporate money laundering could conceivably be achieved, even in such daunting cases as that of BCCI.