

Chapter VI

Financial Institution Requirements

A. Customer Identification and Due Diligence

1. Scope of Customer Identification and Due Diligence
2. Who Is a Customer?
3. Customer Acceptance and Identification Procedures
4. Maintenance and Monitoring of High Risk Accounts
5. Cases calling for Increased Due Diligence
6. Extending Due Diligence to Vendors and Others
7. Insurance Sector Measures
8. Security Sector Measures

B. Suspicious Transaction Reporting

1. Suspicious Transactions: What is involved
2. "Safe Harbor" Provisions for Reporting
3. Insurance Sector Reporting
4. Securities Sector Reporting

C. Record Keeping Requirements

1. Financial Institutions Record-Keeping Requirements
2. Insurance Sector Record-Keeping Requirements
3. Securities Sector Record-Keeping Requirements

D. Cash Transaction Reporting

1. Multiple Cash Transactions
2. Cross-Border Movements
3. Modern Money Management Techniques

E. Privacy Laws Versus Reporting and Disclosure

F. Internal Controls, Compliance, and Audit

It is axiomatic that money launderers and those who finance terrorism must have access to financial institutions. These institutions provide the means for such individuals to transfer funds among other financial institutions, both domestically and internationally. These institutions also provide the means to convert currencies and pay for the assets used in the money laundering and terrorist financing process. The types of financial institutions and their capabilities vary greatly among different countries. Thus, it is necessary for a country to make policy decisions about financial institution requirements based upon the unique features of that country's financial institutions, financial markets, and economy in general. All such decisions, however, should be made with reference to international standards.

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

A. Customer Identification and Due Diligence

In accordance with international standards set by the Basel Committee on Banking Supervision (Basel Committee)¹ and by the Financial Action Task Force on Money Laundering (FATF),² countries must ensure that their financial institutions have appropriate customer identification and due diligence procedures in place. These procedures apply to a financial institution's individual and corporate customers alike. These rules or procedures ensure that financial institutions maintain adequate knowledge about their customers and their customers' financial activities. Customer identification requirements are also known as "Know your customer" (KYC),³ a term employed by the Basel Committee.⁴

KYC policies not only help financial institutions detect, deter, and prevent money laundering and terrorist financing, they also confer tangible benefits on the financial institution, its law-abiding customers, and the financial system as a whole. In particular, KYC practices:

- promote good business, governance, and risk management among financial institutions;
- help maintain the integrity of the financial system and enable development efforts in emerging markets;
- reduce the incidence of fraud and other financial crime; and
- protect the reputation of the financial organization against the detrimental effect of association with criminals.⁵

1. Basel Core Principles for Effective Banking Supervision and Customer Due Diligence for Banks, principle 15, at <http://www.bis.org/publ/bcbs30.pdf>.

2. *The Forty Recommendations*, http://www1.oecd.org/fatf/40Recs_en.htm and *Special Recommendations*, http://www1.oecd.org/fatf/SrecTF_en.htm. *The Forty Recommendations* are reprinted in Annex IV and the *Special Recommendations* in Annex V of this Reference Guide.

3. Basel Committee, Core Principle for Effective Banking Supervision, Principle 15 states, "Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know-your-customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements."

4. Basel Customer Due Diligence for Banks states: "Supervisors around the world are increasingly recognizing the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls." <http://www.bis.org/publ/bcbs85.pdf>.

5. Derived from Basel Customer Due Diligence for Banks (provision 9).

Financial Institution Requirements

1. Scope of Customer Identification and Due Diligence

The customer identification and due diligence procedures employed by a financial institution must also apply to its branches and majority-owned subsidiaries—both domestically and internationally—provided local law is not in conflict.⁶ Where local law prohibits implementation, relevant authorities in the home country should be informed that these procedures cannot be applied by their host country institutions. Host country supervisors should make efforts to change such laws and regulations in the local jurisdiction.⁷ Absent any legal restrictions in the host country, when two different levels of regulatory standards exist between the home and host country, the higher or more comprehensive, of the two standards should be applied.⁸

2. Who Is a Customer?

The Basel Committee defines a customer as:

- a person or entity who maintains an account with a financial institution or on whose behalf an account is maintained (i.e., beneficial owners);
- beneficiaries of transactions conducted by professional intermediaries (e.g., agents, accountants, lawyers); and
- a person or entity connected with a financial transaction who can pose a significant risk to the bank.⁹

A crucial aspect of customer identification is establishing whether the customer is acting on his, her or its own behalf, or whether there is a beneficial owner of the account that may not be identified in the documents maintained by the financial institution. If there is any reason to suspect that the customer is acting on behalf of another person or entity, appropriate due diligence measures should be instituted.

6. *The Forty Recommendations*, Rec. 20.

7. *Id.*

8. Basel Customer Due Diligence for Banks (provision 66).

9. *Id.* (provision 21).

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

Beneficial ownership is also difficult in the case of legal entities or corporations where there is tiered ownership involved. Tiered ownership involves one corporation owning or controlling one or more other corporate entities. In some cases, there can be numerous corporations each, in turn, owned by another corporation and, ultimately, owned or controlled by a parent corporation. When corporations or legal entities are involved, appropriate due diligence measures should be employed to determine the identity of the actual parent or controlling entity.

3. Customer Acceptance and Identification Procedures

Financial institutions should develop and enforce clear customer acceptance and identification procedures for clients and those acting on behalf of clients.¹⁰ These procedures should include the development of high-risk-customer profiles. Such profiles would include standard risk indicators such as personal background, country of origin, possession of a public or high-profile position, linked accounts, and type and nature of business activity.¹¹

When crafting customer acceptance policies, financial institutions must take great care to strike the appropriate balance between risk aversion regarding criminal activities and the willingness to take on new clients. As a general rule, the rigidity of the acceptance standards should be commensurate with the risk profile of a potential customer. It is strongly recommended that only senior management should render decisions on customers whose profiles suggest they pose a high risk of money-laundering activities.¹²

Financial institutions should design their customer acceptance policies so that the socially disadvantaged are not excluded. Nor should these customer acceptance policies in any way restrict the general public's access to financial services.¹³ This is particularly important for countries moving toward a broader use of financial instruments, including the use of checks, credit or debit cards, electronic and other payment mechanisms, and shifting away from a cash-based economy.

10. *Id.* (provision 20).

11. *Id.*

12. *Id.*

13. *Id.*

Financial Institution Requirements

Accounts should be opened only after the new customer's identity has been satisfactorily verified.¹⁴ No customer should be permitted to open or maintain an account using an anonymous or fictitious name. This prohibition also applies to a numbered account if that account is accessed by use of a number or code once the account does not require the customer identification procedures using official documentation.¹⁵ Numbered accounts are only permitted when the same customer identification procedures and supporting documentation (with record keeping) are employed. Under these guidelines, financial institutions must check and verify their customers' official identifying document. The best documents for verifying the identity of potential or actual customers are those that are the most difficult to reproduce.¹⁶ In this regard, countries should require the use of "official" documents issued by appropriate authorities such as a passport, driver's license, personal identification or tax identification document.

In those instances where an agent is representing a beneficiary (e.g., through trusts, nominees, fiduciary accounts, corporations, and other intermediaries), financial institutions need to take reasonable measures to verify the identity and nature of the persons or organizations on whose behalf an account is being opened or for whom a transaction is being completed.¹⁷ Financial institutions need to verify the legality of such entities by collecting the following information from potential customers:

- name and legal form of customer's organization;
- address;
- names of the directors;
- principal owners or beneficiaries;
- provisions regulating the power to bind the organization;
- agent(s) acting on behalf of organization; and
- account number (if applicable).¹⁸

14. *Id.* (provision 22).

15. *The Forty Recommendations*, Rec.10, and *Basel Customer Due Diligence for Banks*, (provision 30).

16. See *Basel Customer Due Diligence for Banks*, (provision 23).

17. *The Forty Recommendations*, Rec. 11.

18. *Id.*, Rec. 10.

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

In cases of fund transfers, such as money remittances, financial institutions should include accurate and meaningful originator information (name, address, and account number) and pass this information along the payment chain with the fund transfer.¹⁹

A client's identity should be confirmed through due diligence procedures in cases where he or she is an occasional customer who has exceeded the designated threshold (see part E of this chapter), or when there is any doubt of that customer's actual identity.²⁰ The same would apply in the event of the occasional corporate customer.

Customer identification is an ongoing process that requires, as a general rule, financial institutions to keep up-to-date records on all relevant client information. Records should be updated in the event, for example, of significant transactions, changes in customer documentation standards, material changes in an account's operation, and the realization that current records are insufficient.²¹ National supervisors are strongly encouraged to assist financial institutions in developing their own customer acceptance and identification procedures.

4. Maintaining and Monitoring of High Risk Accounts

Financial institutions should avoid accounts kept through correspondent financial institutions located in high-risk jurisdictions with lax legal safeguards against money laundering and terrorist financing. The FATF classifies certain jurisdictions as "noncooperative countries and territories" (NCCT).²² These jurisdictions pose special high risk issues for financial institutions.

Similarly, transactions with certain types of "shell banks" should also be avoided. In general, the shell banks to be avoided are those incorporated in a jurisdiction having no physical presence or no affiliation with a regulated financial group.²³

19. See FATF, Spec. Rec. VII.

20. See Basel Customer Due Diligence for Banks, Provision 53, and FATF, *The Forty Recommendations*, Rec. 14.

21. Basel Customer Due Diligence for Bank, Provision 24.

22. For the complete list of FATF's "noncooperative" jurisdictions, see http://www1.oecd.org/fatf/NCCT_en.htm.

23. See Basel Customer Due Diligence for Banks (Provision 51).

Financial Institution Requirements

Financial institutions are strongly encouraged to employ software programs to assist in their management of information.²⁴ Such programs aid in gathering, analyzing, screening, and communicating data that identify high-risk customers and high-risk activities. They should screen out unusual or suspicious activities.²⁵ These programs play a key role in detecting potentially suspicious activity amid the vast number of legitimate daily transactions.

In addition, financial institutions should fine-tune their monitoring capabilities to adjust for multiple international accounts, which are sometimes known vehicles for subtle system abuse conducted on a cross-border basis. Financial institutions should account for this potential for abuse by aggregating and monitoring significant balances and activity in accounts on a “world-wide consolidated basis.”²⁶

5. Cases Calling for Increased Due Diligence

As a general rule, due diligence should be commensurate with an account’s perceived risk level.²⁷ Higher-risk customers and accounts should receive greater scrutiny. Increased diligence should be exercised in the instances identified below:²⁸

- transactions in any way suspected to be related to terrorism or organizations that sponsor or assist terrorism;
- fund transfers that do not offer complete originator information (i.e., name, address, and account number);
- new technology that permits customer or transactional anonymity;
- complex, large, or unusual patterns of transactions with no apparent economic or lawful purpose;
- account activity in jurisdictions known for lax legislation on money laundering and terrorist financing;

24. *Id.*, (provisions 53–54).

25. *Id.*

26. *Id.*, (provision 16).

27. *Id.*, (provision 6).

28. *Special Recommendations*, Spec. Recs. IV and VII; *The Forty Recommendations*, Recs. 9, 13, 14, and 21; and Basel Customer Due Diligence for Banks (provisions 23, 29, 35–36, 44, 46, and 52). This list is illustrative and is not exhaustive of all circumstances calling for increased due diligence.

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

- foreign nationals maintaining accounts in another sovereign absent a clearly expressed reason;
- instances where a financial institution believes another financial institution has refused service to a potential customer;
- business referrals through correspondent banking services (i.e., wire transfers and third-party use of correspondent accounts);
- private banking and high-risk customers, particularly politically exposed individuals and their affiliates; and
- customers who do not present themselves for face-to-face interviews or transactions (e.g., electronic banking via Internet or third-party introduction).

Steps should be taken to mitigate the higher degree of risk posed by such cases. This means obtaining more information about the customer, the account, the institution, the transaction, or the jurisdiction involved. It is standard, for example, for financial institutions to require more information from customers who do not present themselves for face-to-face interviews; such unconventional transactions can be cleared once that additional information is provided.²⁹ The customer can provide such additional information in the form of certified documents, additional forms of identification, an independent and verifiable customer contact, third-party or institutional referrals that meet KYC standards, or a customer first payment under his or her name at another bank adhering to similar standards.³⁰

If the customer is not able to supply sufficient information to address the due diligence concerns of a financial institution or if suspicions persist, the institutions should retain the authority not to accept the customer. In this regard, care must be taken to establish the specific reasons for denying service so as not to subject the institutions to potential legal liability. However, the authority to deny service for failure to furnish appropriate customer identification information should be available as an option to institutions.

29. Basel Customer Due Diligence for Banks (provision 48).

30. *Id.*

Financial Institution Requirements

6. Extending Due Diligence to Vendors and Others

The supply-chain structure of many businesses has become increasingly complex and interconnected with the advance in global commerce. Consequently, many financial institutions have found it necessary to exercise greater diligence over the vendors, suppliers, and agents of organizations as well as with employees and correspondent banks of financial institutions. Each country's national supervisor may wish to consider implementing policies that incorporate these trends in due diligence.

7. Insurance Sector Measures

The International Association of Insurance Supervisors (IAIS) maintains its own guidelines for customer identification and due diligence; the insurance industry must adhere to these in addition to the relevant guidelines above. The IAIS guidelines recommend that insurance companies:

- establish to their “reasonable satisfaction” that every party relevant to the insurance application actually exists. For large numbers of subjects (e.g., group life policies and pensions), it may be sufficient to use a limited group such as the principal shareholders or main directors;
- verify all underlying principals as well as their relationship with the policyholders—the principals and not the policyholders should be questioned regarding the nature of the relationship;
- prohibit anonymous and fictitious accounts;
- verify claims, commissions, and other money administered to nonpolicyholders (e.g., partnerships, companies);
- increase due diligence when the policyholder's financial flows or transaction patterns change in significant, unexpected, or unexplained ways;
- increase due diligence regarding the purchase and sale of second-hand endowment policies and the use of single-unit-linked policies; and
- monitor reinsurance or retrocession on a regular basis as a way to ensure payments to *bona fide* reinsurance entities at rates justified by the risk level.³¹

31. See IAIS, Anti-Money Laundering Guidance Notes, <http://www.iaisweb.org/framesets/pas.html>.

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

8. Security Sector Measures

The International Organization of Securities Commissions (IOSCO) has not established separate customer identification or due diligence requirements for securities firms, brokers, or collective investment entities. Although IOSCO has not established such specific requirements, the customer identification requirements of *The Forty Recommendations* (as described more fully in the Methodology) do apply to the securities sector.

B. Suspicious Transactions Reporting

“Employees should be required to report suspicious or unusual behavior to a superior or to internal security.”³² Financial institutions have an obligation, in other words, according to this international mandate, to report suspicious transactions. “Moreover, banks should be required to report suspicious activities and significant incidents of fraud to the supervisors, [and] supervisors do need to ensure that appropriate authorities have been alerted.”³³ Institutions reporting suspicious activity should not in any case notify their customers that their behavior has been reported as suspect to authorities.³⁴ From that point on—which is to say, upon notification—financial institutions must fully comply with instructions from government authorities.³⁵

1. Suspicious Transactions: What Is Involved

Suspicious transactions have certain broad characteristics, including, most obviously, transactions that depart from normal patterns of account activity. Any complex or unusually large transactions—in addition to any unusual patterns of transactions absent an apparent economic, commercial, or lawful purpose—are suspect and, therefore, merit further investigation by the financial institu-

32. *Id.*

33. Basel Core Principle 15, Description 31.

34. *The Forty Recommendations*, Rec.17.

35. *Id.*, Rec.18.

Financial Institution Requirements

tion and, if necessary, by the appropriate authorities.³⁶ To assist financial institutions in screening for suspicious transactions, these financial institutions should establish risk-sensitive limits to monitor particular classes or categories of accounts. Specific examples of suspicious activity (e.g., very high account turnover inconsistent with balance size) are useful for individual financial institutions and should be provided to them in some form by supervisors.³⁷

Financial institutions and their employees should always be vigilant for suspicious transactions. While the following are indications of suspicious transactions, the listing is not exhaustive:

- General Signs
 - Assets withdrawn immediately after they are credited to an account.
 - A dormant account suddenly becomes active without any plausible reason.
 - The high asset value of a client is not compatible with either the information concerning the client or the relevant business.
 - A client provides false or doctored information or refuses to communicate required information to the bank.
 - The arrangement of a transaction either insinuates an unlawful purpose, is economically illogical or unidentifiable.

- Signs Regarding Cash Transactions
 - Frequent deposit of cash incompatible with either the information concerning the client or his business.
 - Deposit of cash immediately followed by the issuance of checks or transfers towards accounts opened in other banks located in the same country or abroad.
 - Frequent cash withdrawal without any obvious connection with the client's business.
 - Frequent exchange of notes of high denomination for smaller denominations or against another currency.
 - Cashing checks, including travelers' checks, for large amounts.
 - Frequent cash transactions for amounts just below the level where identification or reporting by the financial institution is required.

³⁶ *Id.*, Rec.14.

³⁷ *Id.*, Rec.28. See also Basel Customer Due Diligence for Banks, (provision 53).

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

- Signs Regarding Transactions on Deposit Accounts
 - Closing of an account followed the opening of new accounts in the same name or by members of the client’s family.
 - Purchase of stocks and shares with funds that have been transferred from abroad or just after cash deposit on the account.
 - Illogical structures (numerous accounts, frequent transfers between accounts, etc.).
 - Granting of guaranties (pledge, bonds) without any obvious reason.
 - Transfers in favor of other banks without any indication of the beneficiary.
 - Unexpected repayment, without a convincing explanation, of a delinquent loan.
 - Deposit of checks of large amount incompatible with either the information concerning the client or the relevant business.

2. “Safe Harbor” Provisions for Reporting

“Safe harbor” laws help to encourage financial institutions to report all suspicious transactions. Such laws protect financial institutions and employees from criminal and civil liability when reporting suspicious transactions to competent authorities in good faith. These legal provisions should provide financial institutions, and their employees or representatives, protection against lawsuits for any alleged violation of confidentiality or secrecy laws so long as the suspicious report was filed in good faith (i.e., it was not frivolous nor malicious).³⁸

3. Insurance Sector Reporting

The IAIS has established its own set of guidelines for reporting suspicious transactions. The insurance industry should follow these, in addition to the relevant guidelines noted above. Insurance companies should report suspicious activity to the financial intelligence unit or other national centralized

³⁸. *The Forty Recommendations*, Rec. 16.

Financial Institution Requirements

authority. The following are sector-specific cases of suspicious transactions meriting additional investigation:

- unusual or disadvantageous early redemption of an insurance policy;
- unusual employment of an intermediary in the course of some usual transaction or financial activity (e.g., payment of claims or high commission to an unusual intermediary);
- unusual payment method; and
- transactions involving jurisdictions with lax regulatory instruments regarding money laundering and/or terrorist financing.³⁹

4. Securities Sector Reporting

The IOSCO has not established separate suspicious activity reporting requirements for securities firms, brokers, or collective investment entities. Although IOSCO has not established separate or additional requirements in this area, the suspicious activity reporting requirements of *The Forty Recommendations* do apply to the securities sector.

C. Record Keeping Requirements

1. Financial Institutions Recording Keeping Requirements

Financial institutions should keep customer identity and transaction records for a minimum of five years following the termination of an account.⁴⁰ Institutions may be required to retain records for longer than five years if required by regulators. Contents of the records should be made readily available to authorities upon request and, further, be sufficient to permit the prosecution of criminal behavior.⁴¹

Maintaining records is important for both prevention and detection of money laundering and terrorist financing purposes. If a potential customer

39. See IAIS Anti-Money Laundering Guidance Notes.

40. *The Forty Recommendations*, Rec. 12.

41. *Id.*

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

knows that records are being maintained, the customer may not be as likely to try to use the institution for these illegal purposes. Record maintenance also helps detect those involved and provides a financial trail to help competent authorities pursue those involved.

The following information should be included when recording a customer's transaction:

- name of the customer and/or beneficiary;
- address;
- date and nature of the transaction;
- type and amount of currency involved in the transaction;
- type and identifying number of account; and
- other relevant information typically recorded by the financial institution.⁴²

2. Insurance Sector Record Keeping Requirements

The IAIS maintains its own set of record keeping requirements; the insurance entities must adhere to these, in addition to the relevant guidelines of *The Forty Recommendations*. The insurance entity must also obtain the following information (where applicable) when recording a customer's transaction:

- location completed;
- client's financial assessment;
- client's need analysis;
- payment method details;
- benefits description;
- copy of documentation used to verify customer identity;
- post-sale records associated with the contract through its maturity; and
- details of maturity processing and claim settlement (including "discharge documentation").⁴³

Financial institution supervisors must verify that all representatives for insurance companies are licensed under appropriate insurance law and juris-

42. *Id.*

43. See IAIS Anti-Money Laundering Guidance Notes.

diction.⁴⁴ Representatives may retain documents on behalf of an insurance entity, but the integrity of the records rests on the insurance entity as the product provider.⁴⁵ In such cases, a clear division of responsibility between the insurance entity and its representative is necessary.⁴⁶

3. Securities Sector Record Keeping Requirements

The IOSCO has established its own set of record keeping requirements, which securities firms should follow in addition to adhering to the applicable general guidelines listed above. IOSCO requires that the national centralized authority on financial crime or other competent authority ensure that intermediaries maintain records as needed demonstrating their adherence to the regulatory rules.⁴⁷ These records should be legible, understandable, and comprehensive, and should include all transactions involving collective investment assets and transactions.⁴⁸

D. Cash Transaction Reporting

Countries should consider the possible benefits of requiring all cash transactions that exceed a fixed threshold amount to be reported.⁴⁹ It is not mandatory, however, that a country have such a requirement. Cash transaction reporting has significant resource and privacy implications, which countries need to take into account in considering the issue. Each country or jurisdiction establishes its own reporting threshold based upon its own circumstances. For example, the United States requires that financial institutions record and report to designated authorities all transactions involving currency or bearer instruments in excess of \$10,000.⁵⁰ Such thresholds may be established by statute, or by regulation under the authority of the appropri-

44. *Id.*

45. *Id.*

46. *Id.*

47. See IOSCO Principles for the Supervision of Operators of Collective Investment Schemes (CIS Sept. 1997), available at http://www.iosco.org/docs-public/1997_principles_for_the_supervision.html.

48. *Id.*

49. *The Forty Recommendations*, Rec. 23.

50. See e.g., U.S. Bank Secrecy Act of 1970.

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

ate government supervisory agency. Depending on circumstances in a country, such requirements may also apply to certain businesses such as casinos, antique or automobile dealers, or when large purchases are paid for in cash.

Relevant authorities should take great care in designating a country's threshold level; it must be high enough to screen out insignificant transactions yet low enough to detect transactions potentially connected with financial crime. In addition, countries may wish to add exemptions to reporting requirements for transactions where reporting is burdensome to the system and not particularly productive for enforcement purposes. In addition, certain entities can represent a low risk for engaging in money laundering, and, therefore, may be eligible for exemption. These entities include governments, certain financial institutions or corporations that are reasonably assumed to be corruption-free, and customers that make frequent, large transactions due to the nature of their businesses. Such exceptions should be reviewed on a regular basis to determine if the exception remains appropriate, both as a general rule and for specific entities, under relevant circumstances.

1. Multiple Cash Transactions

Cash reporting requirements also apply to same-day multiple transactions, a practice called "smurfing." If the consolidated transaction amount exceeds the designated reporting threshold, financial institutions need to report the entire series of transactions.⁵¹ This safeguard against smurfing—whereby many individual transactions involving multiple accounts at a financial institution manage to take place just below the country's reporting threshold—is a vital part of the effort to prevent money laundering and terrorist financing. Criminals and terrorists obviously resort to their own countermeasures to avoid detection by software programs. This is why it is absolutely crucial for the relevant authorities to use proactive analysis in detecting criminal and terrorist financial activity.

Of course, a transaction can also be reported as a suspicious transaction that does not meet the threshold or multiple transactions test. For example, a single deposit of 9,900 may be considered suspicious, under various circum-

51. Basel Customer Due Diligence for Banks, (provision 16).

Financial Institution Requirements

stances, when the country has a reporting threshold of 10,000 because it suggests structuring of transactions by a customer in order to evade the reporting requirements.

2. Cross-Border Movements

Money launderers engage in cross border transfers of cash, bearer negotiable instruments and high-value commodities as a scheme for laundering funds. It is important that countries have a mechanism in place to detect when such transfers may be used for money laundering or terrorist financing purposes.

Finance ministers and customs officials should consider establishing a minimum reporting limit for cross-border movements of currency, other negotiable instruments, and high-value commodities (i.e., precious metals or gems). Unusual or suspicious international movement of such goods, their point of origin and destination should be reported to the country's customs service or other appropriate authorities.⁵²

3. Modern Money Management Techniques

The monitoring capabilities of financial institutions and government officials have benefited from the movement away from cash and currency transfers toward checks, payment cards, direct deposit, and book-entry recording of securities. These transactions leave a helpful paper trail when wrongdoing is suspected and permit competent authorities to make investigations. Success in investigations depends upon accurate and complete record keeping. For this reason, the use of these modern money management and payment transfer methods is highly encouraged.⁵³

⁵². *The Forty Recommendations*, Rec. 22.

⁵³. *Id.*, Rec. 24.

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

E. Privacy Laws versus Reporting and Disclosure

The reporting of information, e.g., suspicious transactions and cash transactions, or the disclosure of records by a financial institution to a competent authority, necessarily involves information that is normally treated confidentially under a country's bank secrecy or privacy laws. In requiring the reporting or disclosure of such information for AML and CFT purposes, a country needs to make appropriate exceptions in its privacy laws or otherwise specifically authorize the reporting and disclosure for those limited purposes. FATF recommends that financial institution privacy laws should be drafted so as not to inhibit the implementation of any of its recommendations.⁵⁴

F. Internal Controls, Compliance, and Audit

Countries should require all financial institutions covered by their AML and CFT laws to establish and maintain internal policies and procedures to prevent their institutions from being used for purposes of money laundering and terrorist financing.⁵⁵ Internal policies and procedures will vary among different institutions and different types of institutions, but they should nevertheless all consider the size, scope, and nature of that institution's operation.

Internal procedures include ongoing training that keeps employees informed and up-to-date about developments on AML and CFT. Employee training needs to (1) describe the nature and processes of money laundering and terrorist financing; (2) explain AML/CFT laws and regulatory requirements; and (3) explain an institution's policies and systems with regard to reporting requirements regarding suspicious activity, with emphasis on customer identification, due diligence and reporting requirement.

In addition, financial institutions should screen job applicants for possible intent to use their institutions to launder money and/or to finance terrorism.⁵⁶

⁵⁴. *The Forty Recommendations*, Rec. 2.

⁵⁵. *Id.*

⁵⁶. *Id.*, Recs. 19 and 26.

Financial Institution Requirements

The designation of an AML/CFT compliance officer at the management level, by each financial institution, is the third internal policy recommended.⁵⁷ Such a compliance officer helps to ensure that appropriate management attention is devoted to the institution's compliance efforts.

An audit function is the fourth required internal policy and procedure that needs to be established; the audit function should be separate from the compliance administration function, in order to test and assure the adequacy of the overall compliance function.⁵⁸

⁵⁷. *Id.*

⁵⁸. *Id.*

