

# Chapter VI

## Preventive Measures

### **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. Low and High Risk Accounts and Transactions
5. Circumstances Requiring Increased Due Diligence
6. Extending Due Diligence to Vendors and Others
7. Insurance Sector Measures
8. Security Sector Measures
9. Measures for Designated Non-Financial Businesses and Professions

### **B. Record Keeping Requirements**

1. Financial Institutions
2. Insurance Sector
3. Securities Sector
4. Designated Non-Financial Businesses and Professions

### **C. Suspicious Transaction Reporting**

1. Suspicious Transactions: What is involved
2. "Safe Harbor" Provisions for Reporting
3. Scope of Reporting Obligation
4. Fiscal Crimes
5. Insurance Sector
6. Securities Sector
7. Designated Non-Financial Businesses and Professions

### **D. Cash Transaction Reporting**

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

### **E. Balancing Privacy Laws with Reporting and Disclosure Requirements**

### **F. Internal Controls**

### **G. Regulation and Supervision**

**M**oney launderers and those who finance terrorism use various types of financial institutions and certain non-financial businesses and professionals to help in their criminal activities. In fact, access to such entities and persons is crucial if criminals are to succeed because financial institutions, and other, provide the means to transfer funds to other financial institutions, both domestically and internationally; to exchange currencies, and to convert proceeds of crime into different financial instruments and other assets.

In *The Forty Recommendations on Money Laundering (The Forty Recommendations)*,<sup>1</sup> the Financial Action Task Force on Money Laundering (FATF) has established a number of preventative measures that a country should adopt in the anti-money laundering (AML) area. These preventative measures are applicable to all financial institutions and, on a more limited basis, to designated non-financial businesses and professions. Furthermore,

---

1. [http://www.fatf-gafi.org/pdf/40Recs-2003\\_en.pdf](http://www.fatf-gafi.org/pdf/40Recs-2003_en.pdf).

these preventative AML measures are equally applicable in combating the financing of terrorism (CFT) under FATF's *Special Recommendations on Terrorist Financing (Special Recommendations)*.<sup>2</sup>

Like all of *The Forty Recommendations*, the preventative measures, generally recommendations 5–25, are not recommendations, but mandates for action by a country if that country wishes to be viewed as compliant with international standards in AML and CFT. These mandates for action are also flexible, however, to permit a country to adopt requirements that are consistent with its own economic circumstances, legal system and constitution. Countries may also wish to examine the Methodology for Assessing Compliance with *The Forty* and *Special Recommendations* for further explanation of the requirements.<sup>3</sup>

### **A. Customer Identification and Due Diligence**

In accordance with international standards set by the Basel Committee on Banking Supervision (Basel Committee)<sup>4</sup> and by FATF,<sup>5</sup> countries must assure 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

---

2. [http://www.fatf-gafi.org/pdf/SRecTF\\_en.pdf](http://www.fatf-gafi.org/pdf/SRecTF_en.pdf)

3. [http://www.fatf-gafi.org/pdf/Meth-2004\\_en.PDF](http://www.fatf-gafi.org/pdf/Meth-2004_en.PDF).

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

5. *The Forty Recommendations*, Rec. 5, [http://www.fatf-gafi.org/pdf/40Recs-2003\\_en.pdf](http://www.fatf-gafi.org/pdf/40Recs-2003_en.pdf). *The Forty Recommendations* are reprinted in Annex IV and the *Special Recommendations* in Annex V of this Reference Guide.

identification requirements are also known as “know your customer” (KYC) rules,<sup>6</sup> a term employed by the Basel Committee.<sup>7</sup>

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.<sup>8</sup>

### 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.<sup>9</sup> 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.<sup>10</sup> Absent any legal restrictions in the host country, when two different levels of

---

6. 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.”

7. 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>.

8. Basel Customer Due Diligence for Banks (provision 9).

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

10. *Id.*

regulatory standards exist between the home and host country, the higher or more comprehensive, of the two standards should be applied.<sup>11</sup>

## 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.<sup>12</sup>

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.

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.

---

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

12. *Id.* (provision 21).

### 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.<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup>

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.<sup>16</sup> 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.

Accounts should be opened only after the new customer's identity has been satisfactorily verified.<sup>17</sup> No customer should be permitted to open or maintain an account using an anonymous or fictitious name.<sup>18</sup> 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.<sup>19</sup> Numbered accounts are only

---

13. *Id.* (provision 20).

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.* (provision 22). *The Forty Recommendations*, Rec. 5.

18. *The Forty Recommendations*, Rec.5, and *Basel Customer Due Diligence for Banks*, (provision30).

19. *Id.*

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.<sup>20</sup> 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.<sup>21</sup> 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).<sup>22</sup>

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.<sup>23</sup>

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

---

20. Basel Customer Due Diligence for Banks (provision 23).

21. *The Forty Recommendations*, Rec. 5.

22. *Id.*, Rec. 5.

23. *Special Recommendations*, Spec. Rec. VII.

designated threshold or when there is any doubt of that customer's actual identity.<sup>24</sup> 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.<sup>25</sup> A country's financial institution supervisors are strongly encouraged to assist financial institutions in developing their own customer acceptance and identification procedures.

#### 4. Low and High Risk Accounts and Transactions

The customer due diligence measures described above should be applied in accordance with the risk attached to the type of customer and transaction. This general principle is central to both the FATF Recommendations and the Basel Committee paper on Customer Due Diligence. For higher risk categories, enhanced measures should be taken and some particular cases are discussed below. For lower risk categories, a country may allow its financial institutions to apply reduced or simplified measures. FATF and the Basel Committee have identified some examples of such customers or transactions, but this is not exhaustive and it is a matter for a country's discretion. Examples of such lower risk customers are financial institutions, public companies and government enterprises.<sup>26</sup> Examples of such transactions are pooled accounts, pension schemes, and small scale insurance policies.<sup>27</sup>

Nevertheless, there is an expectation that customers should always be identified and some basic steps taken to verify identity. The reduced or simplified measures might apply to the extent of the verification process and/or

---

24. Basel Customer Due Diligence for Banks, provision 53; and FATF, *The Forty Recommendations*, Rec. 11.

25. Basel Customer Due Diligence for Bank (provision 24).

26. See *The Forty Recommendations*, Interpretive Notes to Rec. 5, paragraphs 9 and 10.

27. See *The Forty Recommendations*, Interpretive Notes to Rec. 5, paragraphs 11 and 12.

the amount of information collected about the purpose and nature of the business relationship and transactions.<sup>28</sup>

A particular issue on which risk is a factor concerns establishing the identity of customers who already had accounts before verification of identity for new customers became a requirement. Neither the Basel Committee nor FATF requires a comprehensive program to be instituted to verify the identity of existing customers or conduct other due diligence measures.<sup>29</sup> However, it is required that financial institutions should verify identity and carry out further due diligence on existing customers depending on materiality and risk.

## 5. Circumstances Requiring Increased Due Diligence

In certain cases, *The Forty Recommendations* provide that certain enhanced due diligence measures should be taken in addition to those performed in the normal course by financial institutions. The following discusses those cases requiring additional due diligence procedures.

### *a. Politically Exposed Persons*

FATF defines Politically Exposed Persons (PEPs) as:

Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of State owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior officials in the forgoing categories.<sup>30</sup>

---

28. See *The Forty Recommendations*, Interpretive Notes to Rec. 5, paragraph 9.

29. See *The Forty Recommendations*, Interpretive Notes to Rec. 5, paragraph 8.

30. *The Forty Recommendations*, Glossary, Politically Exposed Persons.

This definition covers only those customers who have public functions in a “foreign” country. Thus, it does not apply to “domestic” PEPs. However, FATF encourages countries to extend extra due diligence to domestic PEPs, but requires that extra due diligence be applied to foreign PEPs.<sup>31</sup>

The additional due diligence measures consist of the following:

- Identifying PEPs;
- Approval at senior management level to account opening;
- Establishing the source of wealth and funds;
- Enhanced ongoing monitoring.

Actually finding out whether a customer is a PEP is often the biggest challenge for a financial institution given the definition of the term. No official organization issues a list of such individuals, but various commercial entities maintain and regularly update such lists.

#### *b. Cross-Border Correspondent Banking Relationships*

Cross-border correspondent banking relationships are another source of potentially high risk accounts for financial institutions. Such relationships could be a way for entities or persons from countries with lax arrangements to gain access to the global financial system without undergoing proper due diligence procedures. Before entering into correspondent banking relationships with a cross-border institution, a bank should:

- Establish the nature of the respondent bank’s business, its reputation, and the quality of its supervision;
- Assess the AML/CFT controls of the respondent bank;
- Obtain senior management approval for the relationship;
- Document respective responsibilities;

---

31. *The Forty Recommendations*, Interpretive Notes to Rec. 6.

- If “payable-through-accounts” are to be a feature of the business relationship, assure that the respondent bank verifies the identity and conducts ongoing due diligence of its customers.<sup>32</sup>

Correspondent banking relationship with institutions located in countries classified by FATF as “non-cooperative countries and territories” (NCCTs) should be avoided.<sup>33</sup> No transactions should be undertaken with “shell banks” (i.e., a bank that is incorporated in a jurisdiction in which it has no physical presence and that is not affiliated with a regulated financial group).<sup>34</sup>

### *c. Non Face-to-Face Customers*

As technology develops, the phenomenon of “non face-to-face” customers and business relationships is growing as customers use the telephone and internet to obtain financial services without necessarily visiting the provider. There is no intention on the part of the international standard setters to obstruct such developments, which give customers greater choice and services as well as benefit the economy. Financial institutions and others providing such services need to be aware that the AML/CFT risks are rather different with respect to such customers and need to take appropriate steps to deal with them.<sup>35</sup>

While FATF raises the issue of increased risk with such accounts, it does not provide any guidance on which steps should be taken to address such increased risks. Thus, it is left to each country’s discretion to establish appropriate policies and procedures.

---

32. *The Forty Recommendations*, Rec. 7.

33. For the complete list of FATF’s “no cooperative” jurisdictions, see [http://www.fatf-gafi.org/NCCT\\_en.htm](http://www.fatf-gafi.org/NCCT_en.htm).

34. *The Forty Recommendations*, Rec. 18. See also Basel Customer Due Diligence for Banks (Provision 51).

35. *Id.*, Rec. 8.

#### *d. Introduced Business*

In some countries, financial businesses have customers “introduced” to them by intermediaries or third parties and will not have carried out any due diligence on these customers. In such circumstances, financial institutions should do three things.<sup>36</sup> First, the institution should make sure that the introducer is subject to customer due diligence requirements and that its compliance with such due diligence requirements is subject to supervision. Second, the institution should make certain that the introducer has collected sufficient information about identity and other relevant due diligence documentation about the customer. Third, the institutions should make sure that the introducer can make that information available on request without delay.

The introducer can be domestic or international. Where it is an international party that is the introducer, the financial institution needs to be especially vigilant that the above requirements are met. Several countries, which permit introduced business, require that the introducer should be an individual or an institution that is subject to AML controls, is supervised by a regulatory body with responsibility for compliance with AML controls, and is located in a country that complies with FATF standards.

#### *e. Other High Risk Business*

FATF also draws attention to two other categories of transactions that require special attention. First, there are complex, unusual large transactions and unusual patterns of transactions which have no apparent economic or visible lawful purpose.<sup>37</sup> The background and purpose of such transactions should, as far as possible, be examined and the findings recorded. Where the financial institution cannot discover such information and/or is uneasy about the business, it should consider declining the business and/or making a suspicious transaction report.

---

36. *Id.*, Rec. 9.

37. *Id.*, Rec. 11.

Second, there are countries that have been identified as non-compliant with FATF recommendations that merit special attention. While transactions with such countries are not prohibited, financial institutions should pay special attention to them and, when there is doubt about their purpose, investigate further and record the outcome.<sup>38</sup> If the financial institution is not satisfied that the transaction is *bona fide* it should consider declining the business and/or making a suspicious transaction report.

## 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 financial institution supervisors may wish to consider implementing policies that incorporate these trends in due diligence, especially when such relationships may be considered higher risk as described above.

## 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 requirements of *The Forty Recommendations* discussed 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

---

<sup>38</sup>. *Id.*, Rec. 21.

(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 no policyholders (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.<sup>39</sup>

## 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<sup>40</sup>) do apply to the securities sector.

## 9. Measures for Designated Non-Financial Businesses and Professions

These requirements for customer due diligence, as well as those relating to record keeping, apply to designated non-financial businesses and professions in a more limited manner than to financial institutions. The following discus-

---

39. See IAIS, Anti-Money Laundering Guidance Notes, <http://www.iaisweb.org/02money.pdf>.

40. [http://www.fatf-gafi.org/pdf/Meth-2004\\_en.PDF](http://www.fatf-gafi.org/pdf/Meth-2004_en.PDF).

sion outlines the applicable circumstances where due diligence procedures apply to these entities and persons.

*a. Casinos*

Due diligence procedures for financial institutions apply when casino customers engage in financial transactions equal to or exceeding USD/EUR 3000. Examples of such transactions include buying or cashing-in casino chips, opening accounts, wire transfers, and currency exchange. This does not mean that every gambling transaction has to be monitored or recorded for 5 years.<sup>41</sup>

*b. Real Estate Agents*

Transactions for a client concerning the buying and selling of real estate require due diligence procedures. However, identification and other customer due diligence need only be conducted when a transaction takes place and only with respect to the party who is the client of the estate agent.<sup>42</sup> In many countries, the client will be the seller, rather than the buyer.

*c. Dealers in Precious Metals and Stones*

Cash transactions, equal to or exceeding USD/EUR 15,000, are to be covered by the due diligence requirements.<sup>43</sup>

---

41. *The Forty Recommendations*, Rec. 12, paragraph a. The applicable recommendations are Recs. 5,6, and 8–11.

42. *Id.*, Rec. 12, paragraph b.

43. *Id.*, Rec. 12, paragraph c.

*d. Lawyers, Notaries, Other Independent Legal Professional, and Accountants*

Identification and due diligence requirements apply to transactions prepared or carried out for a client with respect to the following specific activities:

- Buying and selling of real estate;
- Managing of client money, securities or other assets;
- Management of bank, savings or securities accounts;
- Organization of contributions for the creation, operation or management of companies;
- Creation, operation or management of legal persons or arrangements, buying and selling of business entities.<sup>44</sup>

The key phrase is “prepare for or carry out transactions.” This means that merely providing advice on how to undertake such a transaction is not covered. Identification and customer due diligence (and record keeping) are required after the professional becomes involved in carrying out the transaction, which includes the preliminary work on drawing up the transaction as well as its execution. These are situations in which lawyers and accountants are functioning as “gatekeepers” to the financial system by providing services that would permit clients to engage in potential money laundering or terrorist financing transactions.

*e. Trust and Company Service Providers*

Due diligence procedures are applicable to transactions for a client prepared for and carried out in relation to the following specific activities:

- Acting as a formation agent of legal persons;
- Acting as (or arranging for anchor person to act as) a director or secretary of a company, a partner of a partnership of a similar position in relation to other legal persons;

---

44. *Id.*, Rec. 12, paragraph d.

- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee or an express trust; or
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.<sup>45</sup>

In some countries the above-described transactions are performed by lawyers. To be consistent with the criteria for lawyers set out above, the relevant test is again “prepare for and carry out,” which excludes merely providing advice, but includes preliminary work on carrying out a specific transaction.

## **B. Record Keeping Requirements**

### **1. Financial Institutions**

Financial institutions should keep customer identity and transaction records for a minimum of five years following the termination of an account.<sup>46</sup> Institutions may be required to retain records for longer than five years if required by their regulators. Contents of the records should be made readily available to authorities upon request and, further, be of sufficient detail to permit the prosecution for criminal behavior.<sup>47</sup>

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

---

45. *Id.*, Rec. 12, paragraph e.

46. *The Forty Recommendations*, Rec. 10.

47. *Id.*

- 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.<sup>48</sup>

## 2. Insurance Sector

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").<sup>49</sup>

Financial institution supervisors must verify that all representatives for insurance companies are licensed under appropriate insurance law and jurisdiction.<sup>50</sup> Representatives may retain documents on behalf of an insurance entity, but the integrity of the records rests on the insurance entity as the

---

48. *Id.*

49. See IAIS Anti-Money Laundering Guidance Notes.

50. *Id.*

product provider.<sup>51</sup> In such cases, a clear division of responsibility between the insurance entity and its representative is necessary.<sup>52</sup>

### 3. Securities Sector

The IOSCO has established its own set of record keeping requirements, which securities firms should follow in addition to adhering to the applicable general requirements of *The Forty Recommendations* discussed 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.<sup>53</sup> These records should be legible, understandable, and comprehensive, and should include all transactions involving collective investment assets and transactions.<sup>54</sup>

### 4. Designated Non-Financial Businesses and Professions

Record keeping requirements for designated non-financial businesses and professions apply in the same circumstances as are applicable to customer identification and customer due diligence requirements.<sup>55</sup> See section A.9, above, Customer Due Diligence and Identification, Measures for Designated Non-Financial Businesses and Professions.

## C. Suspicious Transactions Reporting

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should report its suspicions to the applicable financial intelligence

---

51. *Id.*

52. *Id.*

53. See IOSCO Principles for the Supervision of Operators of Collective Investment Schemes (CIS Sept. 1997), available at <http://www.iosco.org/pubdocs/pdf/IOSCOPD69.pdf>.

54. *Id.*

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

unit.<sup>56</sup> 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.<sup>57</sup> Financial institutions, when filing suspicious activity reports (STRs), should not, under any circumstances, notify a customer that his/her behavior has been reported as suspect to authorities.<sup>58</sup> From that point on—which is to say, upon notification—financial institutions should comply fully with instructions from government authorities, including the production of records.<sup>59</sup>

### 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 institution and, if necessary, by the appropriate authorities.<sup>60</sup> 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.<sup>61</sup>

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:

---

56. *The Forty Recommendations*, Rec. 13.

57. Basel Core Principle 15, Description 31.

58. *The Forty Recommendations*, Rec.14.

59. *Id.*, Recs.10 and 28.

60. *Id.*, Rec.11.

61. *Id.*, Rec. 25; See also Basel Customer Due Diligence for Banks, (provision 53).

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

- 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.
  
- Signs Regarding Transactions on Deposit Accounts
  - Closing of an account followed by 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 guarantees (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 provided that the suspicious report was filed in good faith (i.e., it was not frivolous nor malicious).<sup>62</sup>

## 3. Scope of Reporting Obligation

An STR is a way of alerting authorities to the possibility that a particular transaction could involve money laundering or terrorist financing and should, therefore, be investigated. In most cases, the reporting financial institution will not have evidence that the transaction represents the proceeds of crime, and is less likely to know of what specific crime might be involved. The financial institution will simply be aware that the transaction is unusual and not consistent with the normal type of transaction on the account. Most likely, it will not be aware of the source of the funds or the reason for the transaction and cannot inquire of the customer without the risk of tipping-off the customer. In such situations, the institution should submit a suspicious transaction report and leave it to the authorities to further investigate.

---

62. *The Forty Recommendations*, Rec. 14.

Because reporting institutions will usually not know the underlying basis of the transaction, a suspicious transaction reporting system should base the requirement to report on “suspicion” that funds may be related to a criminal offense. It is not necessary to require the reporting institution to investigate the transaction or have actual evidence that the funds relate to criminal activity.

#### 4. Fiscal Crimes

Some countries do not classify fiscal crimes, such as tax evasion, as a money laundering predicate offense. Thus, laundering the proceeds of tax evasion is not necessarily a money laundering offense. However, financial institutions should still report transactions that they find suspicious and leave it to the authorities to determine whether money laundering is involved. Otherwise, there is a risk that customers would attempt to explain away transactions related to money laundering predicates as the proceeds of tax evasion and pressure institutions not to file STRs.

#### 5. Insurance Sector

The IAIS has established its own set of guidelines for reporting suspicious transactions.<sup>63</sup> The insurance industry should follow these, in addition to the requirements of *The Forty Recommendations* noted above. Insurance companies should report suspicious activity to the financial intelligence unit or other national centralized authority. The following are insurance 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);

---

63. See IAIS Anti-Money Laundering Guidance Notes.

- Unusual payment method; and
- Transactions involving jurisdictions with lax regulatory instruments regarding money laundering and/or terrorist financing.<sup>64</sup>

## 6. Securities Sector

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.

## 7. Designated Non-Financial Businesses and Professions

Under the 2003 revision of *The Forty Recommendations*, designated non-financial businesses and professionals are now required to file suspicious transactions reports, but on a more limited basis than their obligation to identify customers and carry out due diligence.<sup>65</sup>

For lawyers, notaries, other independent legal professionals and accountants, there is only an obligation to file an STR only when they engage in a financial transaction for, or on behalf of, a client. This is narrower than the obligation to identify clients and conduct due diligence upon them in two respects:

- The reporting obligation covers only “financial transactions,” not all transactions; and
- There is a reporting obligation only at the point at which the professional engages in a financial transaction for his or her client.<sup>66</sup>

---

64. *Id.*

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

66. *Id.*, Rec. 16, paragraph a.

There is no obligation to report in legally privileged circumstances. Individual countries determine when such reporting obligations arise, but the privilege normally covers information obtained either in ascertaining the legal position of a client or representing the client in proceedings. Countries may provide that members of this group may report to their respective self-regulatory organizations (SRO), rather than the FIU, provided the SRO cooperates with the FIU.<sup>67</sup>

Dealers in precious metals and precious stones are required to file STRs only when they engage in a cash transaction with a customer equal to or exceeding the USD/EUR 15,000 threshold.<sup>68</sup>

Trust and company service providers are required to file STRs only in circumstances where they engage in transactions on behalf of a client.<sup>69</sup> As a consequence, any transaction, not just a financial transaction, that is suspicious should be reported. The reporting is limited, however, to situations where the trust or company service provider actually carries out the transaction; mere providing advice or preparing a transaction is not reportable.

#### **D. Cash Transaction Reporting**

Countries should consider the possible benefits of requiring all cash transactions that exceed a fixed threshold amount to be reported.<sup>70</sup> 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.<sup>71</sup>

---

67. *Id.*, Interpretive Note to Rec. 16.

68. *Id.*, Rec. 16, paragraph b.

69. *Id.*, Rec. 16, paragraph c.

70. *The Forty Recommendations*, Rec. 19.

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

Other countries require reporting at similar levels. Such thresholds may be established by statute, or by regulation under the authority of the appropriate government supervisory agency. Depending on circumstances in a country, such requirements may also apply to non-financial businesses and professionals, such as casinos, antique or automobile dealers, lawyers, accountants or other situations where 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 cash 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.<sup>72</sup> 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.

---

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

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 circumstances 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.

Authorities 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.<sup>73</sup>

## 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.<sup>74</sup>

---

73. *The Forty Recommendations*, Rec. 19.

74. *Id.*, Recs. 20 and 28.

### **E. Balancing Privacy Laws with Reporting and Disclosure Requirements**

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 specifically provides that financial institution privacy laws should be drafted so as not to inhibit the implementation of any of its recommendations.<sup>75</sup> At the same time, a country needs to build in protections to assure that confidentiality will be observed, except where public policy needs, such as prosecution for money laundering, outweigh the overall need to protect privacy of financial information. By assuring confidentiality and privacy in the overall scheme, a country protects reporting and disclosure from abuse. In doing so, a country encourages maximum cooperation and proper reporting and disclosure by those entities and persons subject to such requirements.

### **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.<sup>76</sup> 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 require-

---

75. *Id.*, Recs. 4 and 28.

76. *Id.*, Rec. 15..

ments; 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.<sup>77</sup> The designation of an AML/CFT compliance officer at the management level, by each financial institution, is recommended.<sup>78</sup> Such a compliance officer helps to ensure that appropriate management attention is devoted to the institution's compliance efforts.

An audit function is also a 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.<sup>79</sup>

## **G. Regulation and Supervision—Integrity Standards**

The foregoing discussions deal with AML and CFT preventative measures that should be applied by national authorities to financial institutions and certain designated non-financial businesses and professions. It is not sufficient for national authorities to impose those requirements in legislation. Countries also need to take measures to ensure that they are implemented in practice. Like many other elements of the international standards, the extent of regulation and supervision should be based on the money laundering and terrorist financing risk to the institution in question. The framework established by the standard setters envisages different types of regulation and supervision for:

- Core Principle Institutions,
- Other Financial Institutions, and
- Designated Non Financial Businesses and Professions.

---

<sup>77</sup>. *Id.*

<sup>78</sup>. *Id.*, Interpretive Note to Rec. 15.

<sup>79</sup>. *Id.*

The regulations and supervision recommendations regarding integrity standards of *The Forty Recommendations* are discussed in detail in Chapter V, under Supervision and Regulation—Integrity Standards.

#### **H. Legal Entities and Arrangements**

Each country should take appropriate measures to prevent the unlawful use of corporations and other forms of legal entities by money launderers and those who finance terrorism.<sup>80</sup> Such measures should include accurate and timely information about the beneficial ownership and control of legal entities; such information should be accessed in an expeditious manner by competent authorities. In addition, in countries where bearer shares of securities are permissible, appropriate measures should be taken to assure that such bearer instruments are not abused for money laundering or terrorist financing purposes.<sup>81</sup>

A country should also take appropriate measures to assure that trust and similar legal arrangements are not misused by those involved in money laundering or terrorist financing.<sup>82</sup> Such preventative measures should include access to details about the settler, trustee and beneficiaries of these types of legal arrangements.<sup>83</sup>

---

80. Id., Rec. 33.

81. Id.

82. Id., Rec. 34.

83. Id.

