Part II

Preventive Measures

Drafting note: Part II sets out preventive measures to be applied by financial institutions and designated non-financial businesses and professions (DNFBPs) to combat money laundering and terrorism financing. There is reference in the text to 'this Act' as it is envisaged that Part II could be adopted as a separate act or together with other parts of the model legislative provisions. Drafting authorities should review the use of the term in the provisions.

The FATF standard generally grants jurisdictions discretion in choosing the legal tool for introducing preventive measures – whether through primary or secondary legislation, or other enforceable means. Certain aspects of the FATF standards, however, must be set out in primary legislation, namely:

(1) the principle of undertaking customer due diligence (CDD);

(2) record-keeping requirements for transactions and CDD information; and

(3) the obligation to promptly report suspicious transactions to the FIU.

It is important to note that the provisions in this model legislation not only introduce the general obligations for financial institution/DNFBPs to apply due diligence, keep records and file suspicious transaction reports (STRs), but prescribe these obligations in great detail. Drafting authorities may thus choose to include some of these detailed provisions in secondary legislation, regulations or other enforceable instruments rather than to address them through primary legislation. This approach would provide for a greater level of flexibility should an amendment to the relevant requirements become necessary.

Section 3 Definitions

(1) The following definitions shall apply in this Part:

Account means any facility or arrangement by which a financial institution or a DNFBP does any of the following:

(a) accepts deposits of funds;

(b) allows withdrawals or transfers of funds;

(c) pays negotiable or transferable instruments or other orders, or collects negotiable or transferable instruments or payment orders on behalf of any other person; or

(d) makes any facility or arrangement for a safety deposit box or for any other form of safe deposit.

Accountable person means a financial institution or a DNFBP.

Bearer negotiable instrument means any monetary instrument in bearer form, such as travellers' cheques; negotiable instruments, including cheques, promissory notes and money orders, that are in bearer form, endorsed without restriction, made out to a fictitious payee or otherwise in such form that title thereto passes upon delivery; or incomplete instruments such as cheques, promissory notes and money orders, signed but with the payee's name omitted.

Beneficial owner means a natural person who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted, or any person who exercises effective control over a legal person or legal arrangement.

Business relationship means an association between individuals and/or companies entered into for any commercial purpose.

Correspondent relationship means the provision of banking, payment, cash management, international wire transfers, cheque clearing, payable through accounts, foreign exchange, securities transactions, funds transfer or similar services by one financial institution (the correspondent institution) to another financial institution (the respondent institution).

Drafting note: Under the revised FATF standard the requirements for correspondent banking relationships were expanded to cover also 'other, similar relationships', for example those established for securities transactions or funds transfers. The definition should reflect this change.

For further information on correspondent banking see *The Wolfsberg Group – Wolfsberg Anti-Money Laundering Principles for Correspondent Banking 2014.*

Currency or money means coin and paper money of any jurisdiction that is designated as legal tender or is customarily used and accepted as a medium of exchange, including virtual currency as a means of payment.

Drafting note: The definition of currency should be drafted to cover both domestic and foreign currency and should include a reference to virtual currencies. During the process of updating the model legislative provisions, the FATF Guidance on Virtual Currencies was published. In brief, the FATF guidance adopts the approach that AML/CFT frameworks may indirectly apply to persons using virtual currencies for commercial purposes when they interact with the established finance system. The FATF guidance makes clear that persons and institutions that facilitate interaction or exchange between virtual currency and the established finance system should be subject to existing AML/CFT regimes.

Customer means any of the following:

(a) the person for whom a transaction or account is arranged, opened or undertaken;

(b) a signatory to a transaction or account;

(c) any person to whom an account or rights or obligations under a transaction have been assigned or transferred;

(d) any person who is authorised to conduct a transaction or control an account;

(e) any person who attempts to take any of the actions referred to in (a) to (d) above; or

(f) such other person as may be prescribed by regulation by the [minister/competent authority].

DNFBPs means any of the following:

(a) casinos, including internet casinos and ship-based casinos;

(b) real estate agents;

(c) dealers in precious metals and dealers in precious stones when they engage in any currency transaction equal to or above [designated amount];

> **Drafting note:** The FATF-designated threshold for dealers in precious metals and dealers in precious stones is EUR/US$5,000. Jurisdictions may, however, set a lower threshold if this is deemed necessary in the specific jurisdictional context to properly mitigate the risks of money laundering or terrorism financing through these sectors.

(d) lawyers, notaries, other legal professionals, and accountants when they prepare for, engage in, or carry out transactions for a client concerning any of the following activities:

(i) buying and selling of real estate;

(ii) managing of client funds or securities;

(iii) management of bank, savings or securities accounts;

(iv) organisation of contributions for the creation, operation or management of legal persons;

(v) creation, operation or management of legal persons or legal arrangements, and buying and selling of business entities;

> **Drafting note:** Drafting authorities shall ensure that the definition under (d) is sufficiently comprehensive to include any regulated professionally-qualified individual undertaking transactional work.

(e) trust and company service providers (TCSPs) not otherwise covered by this Act which, as a business, prepare for or carry out or otherwise provide the following services or transactions to third parties:

(i) acting as a formation, registration or management agent of legal persons;

(ii) acting as, or arranging for another person to act as, a director or secretary of a company or a partner of a partnership, or to hold a similar position in relation to other legal persons;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or legal arrangement;

(iv) acting as, or arranging for another person to act as, a trustee of an express trust or performing the equivalent function for another, similar form of legal arrangement;

(v) acting as, or arranging for another person to act as, a nominee shareholder for another person;

(f) such other businesses and professions as may be prescribed by regulation by the [insert name of minister/competent authority].

Drafting note: Businesses and professions listed under items (a) to (e) are covered by the FATF definition DNFBPs and thus must be covered by jurisdictions' AML/CFT requirements.

Item (f) of the definition includes the possibility of designating additional categories of DNFBPs if a particular jurisdiction identifies other service providers that either act as gatekeepers to the financial sector or may be used for money laundering or terrorism financing purposes. Examples of such additional categories are gaming and gambling houses, auction houses and lotteries, as well as businesses that sell high-value goods such as car dealerships. Although the FATF standard does not mandate the expansion of AML/CFT frameworks beyond those categories specifically covered under items (a) to (e) above, jurisdictions may nevertheless find it necessary or useful to do so. In making this policy choice, however, the need to mitigate existing risks needs to be carefully balanced against the oftentimes limited resources available to governments and individual authorities to ensure effective implementation of the law.

For subsection (e) relating to TCSPs, the phrase 'another, similar form of legal arrangement' is included to cover legal arrangements such as the administration of a Stiftung under German, Austrian, Swiss or Liechtenstein law. Although such structures are not used in common law jurisdictions, TCSPs in common law jurisdictions may be involved in forming or advising on or administering such arrangements.

Document means a record of information kept in any form, including in electronic format.

Financial institution means any person that conducts as a business one or more of the following activities or operations for or on behalf of a customer:

(a) acceptance of deposits and other repayable funds from the public, including private banking;

(b) lending, including, but not limited to, consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfeiting;

(c) financial leasing other than with respect to arrangements relating to consumer products;

(d) money or value transfer services;

(e) issuing and managing means of payment, including, but not limited to, credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and electronic money;

(f) issuing financial guarantees and commitments;

(g) trading in (i) money market instruments, including, but not limited to, cheques, bills, certificates of deposit and derivatives; (ii) foreign exchange; (iii) exchange, interest rate and index instruments; (iv) transferable securities; and (v) commodity futures trading;

(h) participation in securities issues and the provision of financial services related to such issues;

(i) individual and collective portfolio management;

(j) safekeeping and administration of cash or liquid securities on behalf of other persons;

(k) otherwise investing, administering or managing funds or money on behalf of other persons;

(l) underwriting and placement of life insurance and other investment-related insurance, including insurance intermediation by agents and brokers;

(m) money changing; and

(n) carrying on such other activity, business or operation as prescribed by regulation by the minister/competent authority.

Drafting note: The term 'financial institution' can be defined by describing either the types of financial activities or the types of businesses. The model provision above adopts the former approach. One important advantage to defining the term through reference to the types of financial activities, as the recommended language suggests, is that the definition also covers persons engaged

(*continued*)

(*continued*)

in the relevant activity but not registered or otherwise formally recognised (for instance, an unregistered bank).

Whichever approach is chosen, it is important that all persons or businesses that perform any of the activities described above be covered by the statutory definition of 'financial institution'. If authorities decide to define the term through reference to the types of businesses, the list should contain a catch-all provision to capture any other entities that carry out the functions noted in the list above. The relevant definition may read along the following lines:

(a) banks and other credit institutions;

(b) life insurance and investment-related insurance companies, insurance underwriters, and insurance agents and brokers;

(c) investment banks and firms;

(d) brokerage firms;

(e) mutual funds and collective investment schemes;

(f) mortgage companies;

(g) commercial and consumer credit companies;

(h) persons that issue, manage or operate credit and/or debit card facilities;

(i) leasing and/or finance companies other than companies that engage solely in financial leasing for consumer products;

(j) funds management companies;

(k) cheque cashers and sellers or redeemers of travellers' cheques, money orders or other monetary instruments;

(l) any person that engages in the purchase, sale or conversion of currency as a business;

(m) any person that engages in funds transfers as a business;

(n) any person providing facilities for the safekeeping of cash or liquid securities on behalf of other persons;

(o) any other person that conducts as a business one or more of the following activities for or on behalf of a customer: (authorities should insert a list compatible with the FATF 40 list of functions); or

(p) any such other activity, business or operation as prescribed by regulation by the minister/competent authority.

Funds or **property** means assets, economic resources, property of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, wherever located, legal documents or instruments in any form, electronic or digital, evidencing title to, or interest in, such assets, economic resources or property, including but not limited to currency, bank credits, deposits and other financial resources, travellers' cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit, and any interest in, dividends or other income on or value accruing from or generated by, in full or in part, any such assets, economic resources or property.

> **Drafting note:** The definition of 'property' or 'funds' combines all elements of the definitions of 'property' and 'funds or other assets' from the glossary to the FATF 40 Recommendations; of 'property' as set out in the Vienna, Palermo and Merida Conventions; and of 'funds' as set out in the Terrorism Financing Convention. Thus, the definition comprehensively covers the requirements under all these instruments.

Funds transfer: see **Wire transfer.**

Legal arrangement refers to express trusts or other similar legal arrangements.

Minister means the [the minister of (name Department or Ministry) or minister responsible for (specify)].

Money laundering means any offence referred to in Part IV, Section 36.

Originator means the person who allows a wire or funds transfer from his/her account, or, where there is no account, the person that places the order with a financial institution to perform a wire or funds transfer.

Payable through account means a correspondent account used directly by a third-party customer of the respondent institution to transact business on such party's own behalf or on behalf of another person.

Person means any natural or legal person.

Politically exposed person (PEP) means a domestic PEP, a foreign PEP or a person who has been entrusted with a prominent function by an international organisation, and includes family members and close associates of any of PEP.

A **domestic PEP** is an individual who is or has been entrusted domestically with a prominent public function, for example head of state or of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation or important political party official.

A **foreign PEP** is an individual who is or has been entrusted with a prominent public function by a foreign jurisdiction, for example head of state or of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, or important political party official.

Persons who have been entrusted with a prominent function by an international organisation are members of senior management of such an organisation, including directors, deputy directors and members of the board or equivalent functions.

Drafting note: The examples of who qualifies as a PEP are likely to be subject to particular local variations, depending on the political and social structures of a jurisdiction, but must always include any person who has been elected or otherwise appointed to a position that allows him or her to influence or direct how a state contracts or invests, or how a state's resources are applied. The term is not intended to cover middle-ranking or more junior individuals in the categories mentioned in the definitions.

The FATF standard requires that the definition of PEPs shall also apply to family members and close associates but does not define the terms 'family members' or 'close associates.' It is thus up to each jurisdiction to define these terms based on local customs and social structures. Typically jurisdictions would cover within the definition of 'family member' any of the following: the spouse or any person considered equivalent to the spouse; children and their spouses or persons considered equivalent to their spouse; parents; siblings; and cousins. The term 'close associate' would usually cover any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements or who is in a close business relations with a PEP, or who has sole beneficial ownership of a legal entity or legal arrangement that is known to have been set up for the benefit *de facto* of a PEP.

Proceeds and **Proceeds of crime** mean any funds or property derived from or obtained, directly or indirectly, as a result of [***Option:*** *or in connection with*] the commission of a criminal offence, including economic gains and funds or property converted or transformed, in whole or in part, into other funds or property.

Drafting note: The optional language ('in connection with') is designed to capture those instances in which the conduct is partially responsible for the proceeds and not solely responsible for the proceeds. Adding this phrase expands the concept of 'proceeds', and makes it clear, for example, in the case of a standalone money laundering prosecution, where there is no prosecution for the predicate offence, that the funds being laundered and which are viewed as proceeds of the predicate offence can also be viewed as proceeds obtained 'in connection with' the money laundering offence.

Property: see **Funds.**

Record means any material on which information is recorded or marked and which is capable of being read or understood by a person, or by an electronic system or other device.

Senior management means an officer or employee with sufficient knowledge of the institution's money laundering and terrorism financing risk exposure and sufficient seniority to make decisions affecting its risk exposure. It need not, in all cases, involve a member of the board of directors and includes a person responsible for compliance or duly authorised to bind the accountable person.

Shell bank means a bank that has no physical presence in the jurisdiction in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. 'Physical presence' means meaningful mind and management located within a jurisdiction. The existence of a local agent or low-level staff does not constitute physical presence.

Suspicious transaction report means a report required to be made under Section 17(1) of this Act.

Terrorism financing means any offence referred to in Part IV, Section 37.

T**ransaction** means a purchase, sale, loan, pledge, gift, transfer, delivery or other disposition, or the arrangement thereof, and includes but is not limited to:

(i) opening of an account;

(ii) any deposit, withdrawal, exchange or transfer of funds, whether in currency or by cheque, payment order or other instrument or by electronic or other non-physical means;

(iii) the use of a safety deposit box or any other form of safe deposit;

(iv) entering into any fiduciary relationship;

(v) any payment made or received in satisfaction, in whole or in part, of any contractual or other legal obligation;

(vi) any payment made in respect of a lottery, bet or other game of chance;

(vii) establishing or creating a legal person or legal arrangement; and

(viii) such other transaction as may be prescribed by the [minister/competent authority] by regulation.

Virtual currency is a digital representation of value that can be digitally traded and functions as:

(i) a medium of exchange; and/or

(ii) a unit of account; and/or

(iii) a store of value that does not have legal tender status or carry any security or guarantee in any jurisdiction.

Wire transfer or **funds transfer** means any transaction carried out on behalf of an originator through a financial institution (including an institution that originates the wire transfer and an intermediary institution that participates in completion of the transfer) by electronic means with a view to making an amount of funds available to any person at another financial institution.

Unless there is a suspicion of money laundering or terrorism financing, in which case the full range CDD measures must be applied without regard to any monetary threshold, Sections 4(3), 5, 6, 7, 9, 10, 12 and 13(1) of this Act shall apply to:

(a) casinos only when a customer opens an account or engages in a financial transaction equal to or above [the designated amount], whether conducted as a single transaction or as several transactions that appear to be linked; and

(b) real estate agents when they are involved in financial transactions for their client concerning the buying or selling of real estate, and with respect to both the vendors and purchasers.

Drafting note: The FATF-designated threshold for casinos is EUR/US$3,000. Below this amount jurisdictions may but are not required to oblige casinos to apply the full range of CDD measures. As the methodology to the FATF 40 Recommendations at Criterion 22.1(a) (footnote 44) notes, the practice of customer identification at entry to a casino could but is not necessarily sufficient. Jurisdictions must require casinos to ensure that they are able to link CDD information for a particular customer to the transactions made by that customer in the casino.

There are no thresholds or limitations with respect to lawyers, other legal professionals or TCSPs. Such professionals must always identify and verify, regardless of threshold, whenever the activity they are engaging in comes within the definition of a DNFBP. When they are not engaged in such activities, they are not covered by the model provisions.

For dealers in precious metals and dealers in precious stones, the FATF provides a threshold of EUR/US$15,000 and dealers are subject to the AML/CFT obligations only with regard to cash transactions exceeding this amount. Since the designated threshold is the same under Recommendations 22 and 23, it is more practical to incorporate it as part of the definitions in Section 3(1).

The [insert name of minister/competent authority] may make regulations for the implementation of the provisions of this Act.

Section 4 Risk Assessment

(1) An accountable person shall identify, assess and monitor its money laundering and terrorism financing risks.

(2) Such measures shall take into account customer, geographic area, product, service, transaction and means of delivery risk factors and shall be proportionate to the nature and size of the accountable person's business and take into account the outcome of any risk assessment carried out at a national level, and any regulatory guidance issued.

(3) An accountable person shall document the risk assessment in writing, keep it up to date and make it available to relevant competent authorities [***option:*** *and SRBs*] upon appropriate request.

(4) Prior to the launch of a new product or business practice or the use of a new or developing technology, an accountable person shall identify and assess the money laundering or terrorism financing risks that may arise in relation to such new products or business practices, or new or developing technologies for both new and pre-existing products, and take appropriate measures to manage and mitigate these risks.

Drafting note: The revised FATF standard reflects a risk-based approach to preventive measures, on an ongoing basis. Accountable persons are expected to identify, assess and understand the money laundering/financing terrorism risks to which they are exposed and to take measures commensurate to those risks in order to mitigate them effectively.

The risk assessment that accountable persons are required to conduct under FATF Recommendation 1 forms the basis of the risk-based approach. Further risk elements are enshrined throughout the FATF Recommendations, for example in Recommendations 10 (CDD measures), 11 (PEPs), 18 (internal controls and foreign branches and subsidiaries) and 19 (high risk countries).

Accountable persons are likely to require further guidance on the methodology to be applied for carrying out the risk assessment; the types of customer, jurisdiction or geographic area and product, service, transaction or delivery channel risk factors that need to be taken into consideration; and the intervals at which the assessment should be updated, etc. Jurisdictions may opt to provide such guidance through secondary legislation, or sector-specific guidance or recommendations. The examples indicated in the interpretative note to Recommendation 10, paragraphs 15 (for higher risk factors) and 17 (for lower risk factors), should be integrated in this guidance.

Recommendation 15 specifically requires that accountable persons carry out a risk assessment in relation to and prior to launching a new product or business practice, or before using new or developing technologies, and to take appropriate measures to manage any identified risks.

Section 5 Customer Due Diligence Requirements

(1) An accountable person shall not establish or maintain an anonymous account or an account in a fictitious name.

(2) An accountable person shall undertake CDD measures by means of reliable and independent source documents or information, such as a passport, a driver's licence, a national identification document, or in the case of legal persons or legal arrangements, a certificate of incorporation, a certificate of good standing, a partnership agreement or a deed of trust, and in the following circumstances:

Drafting note: Drafters should consider the specific kinds of documents or information that would constitute 'reliable and independent source documents and information' in their country-specific context and add to or delete from the list above. Some jurisdictions have chosen to differentiate between documents to be provided by their nationals and documents to be provided by foreign natural or legal persons. It is also important to specifically state the types of documents that may be considered reliable for purposes of identifying and verifying information pertaining to legal persons and legal arrangements.

Drafters may also opt to set out such level of detail through regulation rather than in primary legislation.

(a) when opening an account for or otherwise establishing a business relationship with a customer;

(b) where a customer who is neither an account holder nor in an established business relationship with the accountable person wishes to carry out:

(i) a transaction in an amount equal to or above [the designated amount], whether conducted as a single transaction or several transactions that appear to be linked or

Drafting note: The FATF-designated threshold for CDD for occasional customers is EUR/US$15,000. Jurisdictions may, however, opt to set a lower threshold if this is considered necessary to properly mitigate national money laundering or terrorism financing risks.

Drafting note: The FATF-designated threshold for CDD on wire transfers is EUR/US$1,000. Owing to the potential terrorism financing threat posed by small wire transfers, however, jurisdictions are encouraged to minimise or even eliminate threshold requirements for wire transfers, taking into account the risks of driving transactions underground and the importance of financial inclusion.

(ii) a wire transfer [in the amount equal to or above the designated amount];

(c) whenever doubts exist about the veracity or adequacy of previously obtained customer identification information;

(d) whenever there is a suspicion of money laundering or terrorism financing involving the customer or the customer's account.

(3) With respect to each customer and business relationship, when applying CDD measures an accountable person shall take into account the outcome of the risk

assessment required to be carried out under Section 4. Where the risks are higher, an accountable person shall conduct enhanced due diligence measures consistent with the risks identified. Where the risks are lower, an accountable person may conduct simplified due diligence measures, unless there is a suspicion of money laundering or terrorism financing or a higher risk may be apparent, in which case enhanced CDD measures shall be undertaken. In all cases, an accountable person shall apply the following CDD measures:

Drafting note: As the methodology to the FATF 40 Recommendations at Criteria 10.17–18 makes clear, although the general rule is that all customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner, there are circumstances where the risk of money laundering or terrorism financing is either higher or lower, and where enhanced CDD may thus be called for or simplified CDD may be reasonable.

Jurisdictions will need to make sure that accountable persons fully understand and correctly apply the risk-based approach to preventive measures. It will be necessary for competent authorities to issue guidance to accountable persons to clarify what enhanced and simplified CDD measures may entail and when they are permissible. To the extent possible, the examples of enhanced and simplified CDD measures as set out in paragraphs 20 and 21 of the interpretative note to FATF Recommendation 10 should be integrated in such guidance.

It should be made clear to accountable persons that, even if the risks identified are lower, CDD measures still have to be applied in all cases. It is only the extent of those measures that may be adjusted in line with the lower risk associated with an individual business relationship or transaction. In addition, it should be emphasised that a lower money laundering or financing terrorism risk for one CDD measure, for example for identification and verification purposes because information on the identity of the customer and the beneficial owner is publicly available, does not necessarily mean that the same customer may automatically be treated as low risk also for all other types of CDD measures, for example for transaction monitoring. Simplified measures are never permissible in case of suspicion of lower money laundering or financing terrorism.

Risk variables such as the purpose of an account or relationship, the level of assets to be deposited by a customer or the size of transactions undertaken, and the regularity or duration of the business relationships also may, either by themselves or in combination, increase or decrease the potential money laundering risks associated with certain business relationships, customers, jurisdictions or geographic areas, products, services, transactions or delivery channels. For example, if business relationships with country A are generally considered low risk, the significant amount of deposits by a national of country A in a specific case may still make this one business relationship high risk and require enhanced CDD measures.

(a) Identify the customer and verify the customer's identity as follows, using reliable, independent source documents, data or information:

> **Drafting note:** FATF Recommendation 10 does not prescribe the types of information that accountable persons must obtain for natural person customers, nor does it prescribe what verification measures must be applied with regards to the various types of customers. Jurisdictions thus have the discretion to develop the relevant requirements on this point and to add or remove from the list suggested under subsections (i) and (ii) below.

(i) for a customer that is a natural person, obtain and verify the full legal and any other names, telephone number and email address, permanent address, date and place of birth, nationality, occupation, public position held and/or name of the employer, official personal identification number or other unique identifier contained in an unexpired official document that bears a photograph of the customer, and signature;

(ii) for a legal arrangement or customer that is a legal person, obtain and verify the name, legal form, status and proof of existence, provisions governing the authority to regulate and bind the legal person or legal arrangement; the names of any director, trustee or other person holding a senior management position in the legal entity or legal arrangement; and the address of the registered office or principal place of business.

(b) Identify and verify the identity of any person purporting to act on behalf of the customer, and verify that such person is properly authorised to act in that capacity.

(c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

(d) Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner so that the accountable person is satisfied it knows who the beneficial owner is. As part of this obligation, an accountable person shall:

(i) For customers that are legal persons, obtain and take reasonable measures to verify:

(a) the identity of any natural person(s) who ultimately owns or controls a legal entity by directly or indirectly owning more than *[applicable percentage threshold]* of the shares or voting rights or ownership interests in the legal person, including through bearer shareholdings, trust arrangements or other means; or

(b) if there is doubt under (a) as to whether the person(s) with controlling ownership interests is(are) the beneficial owner(s), or where no natural person under (a) is identified, the identity of the natural person(s) exercising ultimate effective control over the legal person through other means; or

(c) where no natural persons are identified under (a) or (b), the identity of the natural person(s) who hold(s) the position of senior managing official.

(ii) For legal arrangements, obtain and take reasonable measures to verify:

(a) for trusts, the identity of the settlor, the trustee(s), the protector if any, the beneficiaries or, where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates, and any other natural person directly or indirectly exercising ultimate effective control over the trust, including through a chain of control or ownership;

(b) for other types of legal arrangements similar to trusts, the identity of the natural persons holding equivalent or similar positions as those indicated in (a).

Drafting note: Identifying the beneficial owner means both: (1) where the customer is a legal person, identifying who owns the legal person; and (2) identifying the actual owner of the funds that the customer is depositing or otherwise dealing with. Measures set out under Section 5(3)(d)(i) are to be understood as cascading measures. Each measure shall be used only if the previous one has been applied and did not result in the identification of the beneficial owner.

The FATF Recommendations do not prescribe that a controlling ownership interest in a legal entity must be determined based on a shareholding percentage, nor do they stipulate a specific threshold. They merely note that a beneficial owner is 'any natural person having a controlling ownership interest in a legal person' and footnote 30 under Recommendation 10 states that 'a controlling ownership interest depends on the ownership structure of the specific company but may be based on a percentage threshold.' It is thus within jurisdiction's discretion to decide how 'controlling ownership' shall be defined. However, many jurisdictions have adopted a threshold for determining a controlling ownership interest and, therefore, the model legislative provision also adopts this approach.

It is also for each country to determine what it considers as 'direct' or 'indirect' controlling ownership. Directive 2015/840 of the European Parliament and of the Council on the Prevention of the Use of the Financial Systems for the Purpose of Money Laundering and Terrorism Financing (the fourth EU Directive) defines the concepts of 'direct' and 'indirect' ownership as follows: 'A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership; a shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of one or more natural person(s) or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership.

(c) for life and other investment-related insurance business, in addition to applying regular identification and verification measures to customers and beneficial owners, take the following measures as soon as beneficiaries of life or investment related insurance policies are identified or designated:

(i) for beneficiaries that are identified as specifically named natural or legal persons or legal arrangements, take the name of that person;

(ii) for beneficiaries that are designated by characteristics or class, or by other means, obtain sufficient information concerning the beneficiaries to satisfy the life or investment-related insurance business that it will be able to establish the identity of the beneficiary at the time of the pay-out;

(iii) in all cases, verify the identity of the beneficiaries at the time of the pay-out.

Drafting note: Under the revised FATF standard, there is a specific requirement for accountable persons to apply additional CDD measures in relation to beneficiaries of life and other investment-related insurance business. These requirements can be set out in either primary or secondary legislation or through other enforceable means. The information collected shall be recorded and maintained in accordance with the obligations under Section 10 of the model legislative provisions and, where an accountable person is not able to comply with these additional requirements, it shall consider filing a suspicious transaction report with the FIU.

(4) An accountable person shall apply identification and verification measures under this Section before the opening of an account or establishing of a business relationship, or before carrying out a transaction or wire transfer for a customer. If money laundering or terrorism financing is suspected, or if doubts exist about the veracity or adequacy of previously obtained customer identification information, identification and verification measures shall be completed before the customer may conduct any further business.

(5) The [insert name of minister or competent authority] may prescribe the circumstances in which verification of the customer and beneficial owner identity may be completed as soon as reasonably practicable after the establishment of the business relationship, provided that the accountable person (i) effectively manages the risks of money laundering or terrorism financing and (ii) a delay in verification is essential not to interrupt the normal conduct of the business.

(6) An accountable person shall apply the CDD requirements of this Section to customers and beneficial owners with which it had a business relationship at

the time of the coming into force of this Act. Such measures shall be applied at appropriate times and on the basis of materiality and risk, depending on the type and nature of the customer, the business relationship, products or transactions and taking into account whether and when CDD measures have previously been applied and the adequacy of the data obtained, or as may be prescribed by the [insert name of minister or competent authority] by regulation.

Section 6 Reliance on Identification by Third Parties

(1) *[A financial institution] [A DNFBP] [An accountable person] may rely on third parties to perform CDD measures as required by Section 5(3), subject to the following:*

   (a) *there is no suspicion of money laundering or terrorism financing;*

   (b) *the [financial institution] [DNFBP] [accountable person] relying on the third party shall immediately obtain the necessary information as required under Section 5(3) from the third party, including on the identity of each customer and beneficial owner; and*

   (c) *the [financial institution] [DNFBP] [accountable person] shall take adequate steps to satisfy itself that the third party:*

      (i) *will provide without delay copies of identification information and other relevant documents relating to CDD requirements upon request, and* (ii) *is established in or is subject to the jurisdiction of a State where it is subject to requirements equivalent to those specified in this Act, and* (iii) *is regulated, supervised or monitored as to compliance with and has measures in place for compliance with these requirements; and* the [insert name of minister/competent authority] may prescribe any jurisdiction that he/she considers fulfils the terms of section 6, subsection (1)(c)(ii).

(2) *Notwithstanding any other provision in this subsection, the [financial institution] [DNFBP] [accountable person] relying on the third party shall always remain responsible for compliance with this Act, including CDD and reporting requirements.*

   A [financial institution] [DNFBP] [accountable person] relying on a third party that is part of the same financial group as the [financial institution] [DNFBP] [accountable person] may consider that the requirements under subsections (1) and (2) are met if:

   (a) *the financial group applies CDD and record-keeping requirements and internal controls and measures in accordance with the requirements under this Act;*

   (b) *the implementation of the CDD and record-keeping requirements and internal controls and measures is supervised at the financial group level by a competent authority; and*

   (c) *any higher jurisdiction risk is adequately mitigated by the group's AML/CFT policies.*

Drafting note: Section 6 is not mandatory but may be adopted by jurisdictions. Under FATF Recommendation 17 jurisdictions may opt to permit an accountable person to rely on third parties to conduct customer identification subject to specific qualifications. This Section would provide a legislative base for such a practice. States may choose to grant this option only to financial institutions, only to DNFBPs or to all types of accountable persons.

It is important for states to clarify, through either secondary legislation or guidance, that Section 6 does not apply to outsourcing or agency relationships. In a typical third-party reliance scenario, the third party is a regulated, supervised or monitored financial institution or DNFBP subject to the full range of CDD and record-keeping requirements. The third party will typically have an existing relationship with the customer and applies its own procedures to perform the CDD measures. In comparison, in an outsourcing/agency relationship, the outsourced entity applies CDD measures on behalf of the delegating financial institution or DNFBP and, in the course of doing so, is subject to that financial institution or DNFBP's controls.

Section 7 Politically Exposed Persons

(1) An accountable person shall have in place appropriate risk management systems to determine whether a customer or beneficial owner is a PEP and:

(a) For a foreign PEP shall:

(i) obtain approval from a designated senior manager before establishing or continuing a business relationship with such customer or beneficial owner;

(ii) take reasonable measures to identify the source of wealth and source of funds; and

(iii) conduct enhanced on-going monitoring of the business relationship to permit the accountable person to fulfil his or her obligations under this Act, including all of the CDD and reporting requirements thereof.

(b) For a domestic PEP or person who has been entrusted with a prominent function by an international organisation, apply the measures under subsection (1)(a) in the case of a higher risk.

Drafting note: The international standard does not require the same high level of diligence to be applied to domestic PEPs as to foreign PEPs unless there is a higher risk. Jurisdictions may, however, opt to go beyond this minimum standard and apply all measures under Section 7(1)(a) to all types of PEPs, whether foreign, domestic or international.

(*continued*)

(*continued*)

The definitions of domestic, foreign and international PEPs also encompass those persons who no longer hold the position that resulted in their initial qualification as a PEP. While the FATF standard does not prescribe an end to the status of a PEP and thus requires indefinite application of enhanced CDD measures to such persons and business relationships, many EU countries have taken a different approach and apply enhanced CDD measures to 'former' PEPs for a duration of 12 months from the time when the person stopped being entrusted with a prominent public function. After that time, the application of enhanced CDD is required only for those former PEPs that continue to pose a risk and until such time as the person is deemed to pose no further risk. The fourth EU Directive prescribes enhanced CDD measures for former PEPs that should last for a period of at least 12 months and a risk-based approach thereafter.

(2) An accountable person shall take reasonable measures to determine, prior to the time of pay-out, whether the beneficiary of a life or other investment-related insurance policy or the beneficial owner of the beneficiary of such a policy is a PEP and, in case of a higher risk, shall:

(a) inform senior management before the pay-out of the policy proceeds; and

(b) conduct enhanced scrutiny on the whole business relationship with the policyholder and consider filing a report to [insert name of FIU] in accordance with this law.

Section 8 Identification and Account Opening for Cross-border Correspondent Relationships

(1) When entering into a cross-border correspondent relationship, a financial institution shall, in addition to applying the measures under Sections 5 and 7 above:

(a) identify and verify the identity of the respondent institution with which they enter into a correspondent relationship;

(b) collect sufficient information on the respondent institution to fully understand the nature of its business and activities;

(c) based on publicly available information, evaluate the respondent institution's reputation and the nature of supervision to which it is subject, including whether it has been subject to any money laundering or terrorism financing investigation or regulatory action;

(d) obtain approval from a designated senior manager before establishing a new correspondent relationship;

(e) evaluate the controls implemented by the respondent institution with respect to AML/CFT;

(f) establish an agreement on the responsibilities of each party under the relationship with particular regard to (e) above;

(g) in the case of a payable-through account, ensure that the respondent institution has conducted CDD on its customers that have access to the account, has implemented mechanisms for on-going monitoring with respect to its customers, and is able to provide relevant CDD information to the financial institution upon request; and

(h) in the case of trusts or other legal arrangements that sever legal ownership from beneficial interest, ensure that the beneficial owner has been appropriately identified.

(2) A financial institution shall not enter into or continue a correspondent relationship with a shell bank.

(3) A financial institution shall not enter into or continue a correspondent relationship with a respondent institution that permits its accounts to be used by a shell bank.

Drafting note: The obligations under FATF Recommendation 13 regarding correspondent banking apply only to financial institutions, and not to DNFBPs. The reference here should thus be not to 'accountable persons' but to 'financial institutions'.

Section 9 Inability to Fulfil Customer Identification Obligations

An accountable person that cannot fulfil the requirements of Sections 5–8 of this Act shall not open the account or establish the business relationship, or carry out the transaction, or shall terminate the business relationship. The accountable person shall also consider filing a report to [insert name of FIU] in accordance with this Act.

Provisions on On-going Obligations of an Accountable Person

Section 10 Record-keeping

(1) An accountable person shall maintain all books and records with respect to their customers and transactions in accordance with subsection (2), and shall ensure that such records and the underlying information are available on a timely basis

to [insert name of FIU] [***variant:*** *and insert name of other competent authorities*] or as and when required to be disclosed.

(2) Such books and records shall include, as a minimum:

(a) all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identities of customers and beneficial owners, and records and the results of any analysis undertaken in accordance with the provisions of this Act, all of which shall be maintained for not less than five years after the business relationship has ended;

(b) records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for not less than five years from the date of the transaction;

(c) the record of any findings pursuant to Section 12(1)(a) and related transaction information which shall be maintained for at least five years from the date of the transaction; and

(d) copies of all suspicious transaction reports made pursuant to Section 17 or other reports made to the FIU in accordance with this Act, including any accompanying documentation, which shall be maintained for at least five years from the date the report was made.

Section 11 Internal Controls to Combat Money Laundering and Terrorism Financing

(1) An accountable person shall develop and implement programmes for the prevention of money laundering and terrorism financing. Such programmes shall be approved by senior management and be monitored and enhanced, if and as necessary. The programmes shall be appropriate to the risks identified under Section 4 or [insert name of national authority competent to carry out national risk assessments on AML/CFT] and be proportionate to the nature and size of the accountable person's business, but should at a minimum include the following:

Drafting note: FATF Recommendation 1 requires countries to carry out a national risk assessment for AML/CFT. It may be that one or more authorities are coordinating such a risk assessment at the national level. Reference to any such authority and the risks identified at the national level should be included here to ensure that internal controls take into account not only institutional but also national risks. If jurisdictions adopt the draft provisions under Section 2 of the model legislative provisions, which set up the National Committee and give it the mandate to coordinate the national risk assessment, the reference here should be to 'the National Committee'.

(a) internal policies, procedures and controls to fulfil the obligations pursuant to this Act;

(b) adequate screening procedures to ensure appropriate and high standards when hiring employees;

(c) on-going training for all statutory directors, officers and employees to maintain awareness of the laws and regulations relating to money laundering and the terrorism financing, to assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing and to instruct them in the procedures to be followed in such cases; and

(d) independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with this Act.

(2) An accountable person shall designate a compliance officer at senior management level to be responsible for the implementation and on-going compliance of the accountable person's internal programmes, controls and procedures with the requirements of this Act. The compliance officer shall have unrestricted access on demand to all books, records and employees of the accountable person as necessary to fulfil his or her responsibilities.

(3) Financial groups shall implement group-wide programmes against money laundering and terrorism financing, addressing all aspects under subsections (1) and (2) and including policies and procedures for sharing of information within the group for AML/CFT purposes and for safeguarding the confidentiality and use of the shared information. Such policies and procedures shall be applied to all branches and majority-owned subsidiaries of the financial group. Group-level compliance, audit and AML/CFT functions shall have the power to request customer, account and transaction information from branches and subsidiaries as necessary to fulfil their functions.

(4) The [insert name of minister/competent authority] may prescribe the type and extent of measures an accountable person shall undertake with respect to each of the requirements in this Section, having regard to the risks of money laundering and terrorism financing, the size of the business or profession, and the standards set by relevant professional bodies.

Section 12 On-going Due Diligence

(1) An accountable person shall exercise risk-based on-going due diligence throughout the course of each business relationship, which shall include:

(a) ensuring that documents, data, information and records collected under the CDD process are kept updated and relevant, and undertaking regular reviews of existing records, particularly for higher risk customers;

(b) examining transactions carried out to ensure that they are consistent with the accountable person's knowledge of the customer, the customer's commercial or personal activities and risk profile, and, where necessary, the source of funds; and

(c) ensuring that the obligations pursuant to Act, including for high-risk customers, PEPs and correspondent relationships, are fulfilled at all times.

Section 13 Enhanced Customer Due Diligence

(1) An accountable person shall examine as far as possible the background and purpose of all complex, unusually large transactions and all unusual patterns of transactions that have no apparent economic or visible lawful purpose. Where the risks identified are higher, the accountable person shall apply enhanced CDD measures consistent with the risks identified and increase the degree and nature of monitoring of the business relationship to determine whether those transactions or activities appear unusual or suspicious.

(2) An accountable person shall apply enhanced CDD to business relationships and transactions with customers, beneficial owners or accountable persons from higher-risk jurisdictions identified by the [insert name of competent authority] or the accountable person. Such enhanced measures shall be effective and proportionate to the risks identified.

(3) An accountable person shall take such measures as may be prescribed from time to time by [insert name of minister/competent authority] to counter the risks identified with respect to customers, beneficial owners or accountable persons from high-risk jurisdictions.

Drafting note: FATF Recommendation 19 deals with high-risk countries and sets out two distinct obligations, which are (1) that accountable persons apply enhanced CDD to higher-risk countries; and (2) that countries apply specific countermeasures to high-risk countries that were prescribed by a relevant competent authority. The requirements are addressed in subsections (2) (for enhanced CDD) and (3) (for countermeasures), respectively.

Section 14 Obligations Regarding Wire Transfers

(1) A financial institution, when undertaking wire transfers [***option:*** *equal to or above the designated amount*], shall include accurate originator and beneficiary information as follows, and ensure that such information remains with the wire transfer or related message throughout the payment chain:

> **Drafting note:** FATF Recommendation 16 applies to cross-border wire transfers as well as domestic transfers, including serial and cover payments. However, countries may choose to adopt a *de minimis* threshold for cross-border wire transfers of US$/EUR1,000 or less. Below this threshold, countries may opt to apply slightly less stringent requirements. Instead of including full originator and beneficiary information as outlined in subsection (1), fiscal institutions may be permitted to include only the name of the originator and beneficiary, and an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorism financing.

(a) the full name of the originator;

(b) the account number of the originator or, in the absence of an account number, a unique reference number;

(c) the originator's address or national identity number or customer identification number or date and place of birth;

(d) the name of the beneficiary; and

(e) the beneficiary account number where such an account is used to process the transaction.

(2) The [insert name of minister/competent authority] may by regulation modify the requirements in subsection (1) with respect to:

(a) domestic wire transfers, as long as the regulations provide for full originator information to be made available to the beneficiary financial institution and appropriate authorities by other means; and

(b) cross-border transfers, where individual transfers from a single originator are bundled in a batch file, as long as the regulations provide for the originator's account number or unique reference number to be included, and provided the batch file contains full originator information that is fully traceable in the recipient jurisdiction.

(3) Subsections (1) and (2) shall not apply to transfers executed as a result of credit card or debit card transactions, provided that the credit card or debit card number accompanies the transfer resulting from the transaction, nor shall they apply to transfers between financial institutions acting on their own account.

(4) A financial institution generating a wire transfer shall ensure that:

(a) the transfer contains required and accurate originator and beneficiary information as set out under subsection (1) or (2);

(b) all originator and beneficiary information is kept in accordance with Section 10; and

(c) no wire transfer is executed that does not comply with the requirements under this Section.

(5) A financial institution processing an intermediary element of a wire transfer shall:

(a) ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it;

(b) where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with it a related domestic wire transfer, keep a record for at least five years from the day of the transaction of all the information received from the ordering or other intermediary financial institution;

(c) take reasonable measures to identify cross-border wire transfers that lack full and accurate originator and beneficiary information as required under subsection (1) or (2)(b); and apply risk-based policies and procedures to determine whether to execute, reject or suspend such a cross-border wire transfer and appropriate follow-up action.

(6) A financial institution receiving a wire transfers shall:

(a) verify the identity of the beneficiary of a wire transfer and keep this information in line with the requirements under Section 10; and

(b) take reasonable measures to identify cross-border wire transfers that lack originator and beneficiary information as required under subsection (1) or (2)(b); and apply risk-based policies and procedures to determine whether to execute, reject or suspend such a cross-border wire transfer and appropriate follow-up action.

Section 15 Compliance with Obligations by Foreign Subsidiaries and Branches

An accountable person shall require foreign branches and any subsidiaries over which it has control to implement the requirements of Sections 4–14 of this Act to the extent that the applicable laws and regulations in the jurisdiction where the foreign branch or subsidiary is domiciled so permit. If such laws prevent compliance with these obligations for any reason, the accountable person shall advise its competent supervisory authority.

Section 16 Prohibition against Shell Banks

(1) It shall not be lawful to establish, operate or deal with a shell bank, and any person who establishes, operates or intentionally deals with a shell bank shall be guilty of an offence.

(2) It shall not be lawful for an accountable person to deal with a shell bank in another jurisdiction and any accountable person who intentionally deals with such a shell bank shall be guilty of an offence.

> **Drafting note:** In many jurisdictions a specific provision of this kind will not be necessary as market entry requirements or other administrative or legal requirements are such that a shell bank would not be able to obtain a banking licence and thus be established or operate in that jurisdiction. Compliance with FATF Recommendations 13 and 26 on the issue of shell banks can thus be accomplished through other legislation or administrative requirements and in the absence of a specific prohibition to this effect.

Reporting Obligation Provisions

Section 17 Obligation to Report Suspicious Transactions

(1) Subject to the provisions of subsection (3), an accountable person that suspects or has reasonable grounds to suspect that any funds or property are:

  (a) the proceeds of crime; or

  (b) related or linked to, or are to be used for, financing terrorism or terrorist acts, or by a terrorist or a terrorist organisation or those who finance terrorism shall promptly submit [***option:*** *but not later than [three] working days after forming a suspicion*] a report setting forth the suspicions to [insert name of FIU] and in such cases shall promptly respond to requests from [insert name of FIU] for additional information. This obligation shall apply to both completed and attempted transactions, and regardless of the amounts involved.

> **Drafting note:** States have the option of allowing members of the legal profession to file STR reports through an appropriate professional SRB if concerns over legal privilege obligations would make it difficult to ensure effective reporting by lawyers directly to the FIU. Under FATF Recommendation 23 and its interpretive note, states may permit the initial reporting to the SRB in such instances. The SRB has the obligation to forward, promptly and unedited, the report of the suspicion to the FIU. See also Article 34 of the fourth EU Directive, which, in the case of auditors, external accountants, tax advisors, notaries and other legal professionals, permits reporting to the FIU through a competent SRB, provided the SRB is obliged to promptly forward the information to the FIU in an unedited manner.

(2) An accountable person shall provide [insert name of FIU] with all necessary information upon request, and in accordance with the procedures established by [insert name of FIU].

(3) Notwithstanding subsection (1), lawyers, notaries, other independent legal professionals and accountants are required to submit reports under subsection (1) or provide information under subsection (2) only when:

(a) they engage, on behalf of or for a client, in a financial transaction associated with an activity specified in relation to such professionals under Section 3 of this Act; and

(b) the relevant information upon which the suspicion is based or that is requested by [insert name of FIU] was not received from or obtained on a client:

(i) in the course of ascertaining the legal rights or obligations of their client; or

(ii) in performing their task of defending or representing that client in, or concerning, judicial, administrative, arbitration or mediation proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

Drafting note: The FATF standard limits the requirements for reporting by lawyers, notaries, other independent legal professionals and accountants to instances where the lawyer, notary, professional or accountant is engaging in a financial transaction on behalf of or for a client. Section 17(3) is thus formulated in a narrower fashion than the general reporting obligations set forth in Section 17(1) and also narrower than the obligation to conduct CDD, which extends, additionally, to situations in which the lawyer and client are making preparations for such a transaction. It distinguishes between situations in which legal professionals and accountants become aware of a potentially suspicious transaction in the course of being asked to give professional legal or accounting advice and situations in which professionals actually engage in a transaction for their client and are subject to the reporting obligation.

Under FATF Recommendation 23, and the definition of DNFBPs in these model provisions, the minimum requirement is that lawyers, notaries, other independent legal professionals and accountants report suspicious activity when they engage in transactions for their client in any of five categories of activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

If accountants within the state are subject to the same obligation of secrecy or privilege as lawyers, they are also not required to report a suspicious transaction

(*continued*)

(*continued*)

in the circumstances identified in Section 17(3), and the drafting should reflect local practice.

The above reflects minimum requirements. States are free to expand the definition of a DNFBP to cover lawyers, notaries, accountants, etc. in more instances than are set forth under the five categories above. Any provision adopted, however, should respect the professional secrecy obligations as defined by the state's laws.

(4) *An accountable person shall refrain from carrying out a transaction that it suspects to be related to money laundering or terrorism financing until [insert time period, for instance one business day] after it has reported its suspicion to the [insert name of FIU], except that, where refraining from the carrying out of a transaction is impossible or is likely to frustrate the efforts to investigate a suspected transaction, an accountable person may execute the transaction and shall report its suspicion to [insert name of the FIU] immediately thereupon.*

[***variant***: *If [insert name of FIU] considers it necessary by reason of the seriousness or urgency of the case, it may order the suspension of a transaction for a period not to exceed [insert time period as three business days*].

Drafting note: The above subsection is optional and allows for the postponing of a transaction suspected to involve money laundering or terrorism financing. It provides the FIU with an opportunity to order the suspension of the transaction for a short period, providing time for an investigation and for taking steps to seek a freezing order from judicial authorities.

(5) *Supervisory authorities shall inform [insert name of FIU] if, in the course of their responsibilities, they discover facts that could be related to money laundering or terrorism financing.*

Drafting note: This subsection requires supervisory authorities to advise the FIU of facts that suggest money laundering or terrorism financing. The provision of information by supervisors is not required by the FATF standards but is a best practice that jurisdictions may choose to adopt.

In some jurisdictions the provision for this kind of cooperation between agencies within a state is part of internal regulations rather than a measure set out in primary legislation. A regulation may provide that supervisory authorities shall disclose information that comes to their attention and indicates that a person has been or may be involved in money laundering or terrorism financing.

(6) [Insert name of FIU] shall issue regulations on the procedures for and form in which the reports shall be submitted and shall publish guidance from time to time in order to assist accountable persons to fulfil their obligations under this Section.

Section 18 Obligation to Report Currency Transactions

*An accountable person shall submit promptly [**option:** and not later than after [three] working days] a report to [insert name of the FIU] of any currency transaction in an amount equal to or above [the designated amount], whether conducted as a single transaction or several transactions that appear to be linked.*

Drafting note: Some jurisdictions require financial institutions and DNFBPs to report cash transactions above a certain threshold, and regardless of the existence of any criminal suspicion.

The decision whether or not to adopt such a provision and the appropriate reporting threshold depend on the framework a state adopts to screen for suspicious activity and should take into account the nature and size of the jurisdiction's currency flows. States should take care to ensure that the threshold for the currency reporting requirement is not so low that the FIU is overwhelmed with routine reports and that accountable persons do not use this provision as a justification to avoid checks for suspicious transactions, regardless of the amounts involved.

Section 19 Inapplicability of Confidentiality Provisions

There shall be no liability for any breach of any secrecy or confidentiality provisions in any other law if an accountable person is fulfilling their obligations under this Act.

Drafting note: Depending on how bank secrecy laws and regulations operate within a jurisdiction, there may be a need for a provision that makes clear that bank or professional secrecy is lifted for purpose of an accountable person complying with AML/CFT obligations provided for by this law.

Section 20 Prohibition against Tipping-off

Any accountable person, or any director, partner, officer, principal or employee thereof, who discloses to a customer or a third party that a report under Section 17(1), or other information, is being or has been submitted to [insert name of FIU], or that a money laundering or terrorism financing investigation has begun, is being or has been carried out, except in the circumstances provided for in subsection (2) or when otherwise required by law to do so, commits an offence that shall be punishable by imprisonment of up to [insert imprisonment range] and a fine of up to [insert monetary range], or both.

Subsection (1) does not apply where a disclosure was made in order to carry out any function that a person has relating to the enforcement of any provision of this Act or of any other enactment.

Section 21 Protection of Identity of Persons and Information Relating to Suspicious Transaction Reports

(1) *Except for the purposes of the administration of this Act, no person shall disclose any information that will identify or is likely to identify the person who prepared or made a suspicious transaction report, or handled the underlying transaction.*

(2) *No person shall be required to disclose a suspicious transaction report, or any information contained in the report or provided in connection with it, in any judicial proceeding unless the court is satisfied that the disclosure of the information is necessary in the interests of justice.*

> **Drafting note:** Protecting the identity of the person who makes a report and the information in the report facilitates reporting by persons and entities. The provisions above are not required by the FATF 40 Recommendations, but they are nevertheless advisable to preserve the anonymity and confidentiality of persons making or connected with reports and unless the interests of justice otherwise dictate any information arising from such a report.

Section 22 Exemption from Liability for Good Faith Reporting of Suspicious Transactions

No criminal, civil, disciplinary, administrative or any other related proceedings for breach of banking secrecy, professional secrecy or contract shall lie against an accountable person or his or her directors, principals, officers, partners, professionals or employees who, in good faith, submit reports or provide information in accordance with the provisions of this Part of the Act.

Section 23 Authorities Responsible for Supervision

(1) *Responsibility for supervision of compliance by accountable persons with the requirements of this Part of this Act is as follows: [list authority that will supervise for each kind of financial institution and DNFBP, for example: The Central Bank for xxx, The Ministry for Justice for xxx, The Ministry of Finance for xxx, Ministry of Commerce for xxx, casino supervisory authority for xxx, self-regulated organisations for xxx, etc.]*

> **Drafting note:** A preventive regime must also include provisions that, through one mechanism or another, designate the authorities that are responsible for overseeing compliance by accountable persons with their AML/CFT obligations. In most states, in the case of financial institutions this is the responsibility of the financial supervisory authorities for each kind of institution.
>
> The delineation of the responsibility to oversee for AML/CFT purposes for each specific substantive area may often be found in a state's AML law. This
>
> (*continued*)

(*continued*)

optional provision would set forth such responsibility. The detailed procedures, manner, authority, etc. for oversight will then typically be set forth in the state's banking, securities or insurance and other supervision laws. There it is part of the larger responsibility of oversight for such financial institutions. Similarly, states must have provisions for oversight of each type of DNFBP to ensure compliance with AML/CFT obligations. The provision is set forth as optional as it is needed only if it is determined that, in the context of the particular state, the designation of the supervisory authorities that will have the AML/CFT oversight responsibility should be reflected in law and not regulation or administrative directive.

In addition, sector-specific and other legal provisions within the state should be reviewed to ensure that they provide supervisory authorities with the following powers relevant to the AML/CFT obligations:

- the regulation and supervision of all types of financial institutions and DNFBPs for compliance with AML/CFT obligations, including as appropriate through on-site examinations;
- the authority to compel accountable persons to produce any documents and information, including on the specific domestic and international risks associated with customers, products and services of the accountable person;
- the authority to issue instructions, guidelines or recommendations to assist financial institutions and DNFBPs to comply with their obligations;
- the authority to provide assistance in investigations, prosecutions or proceedings relating to money laundering, predicate offences and terrorism financing;
- the authority to cooperate and enter into sharing arrangements regarding relevant information with other domestic and foreign competent authorities;
- the authority to apply appropriate regulatory or supervisory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a, or participating directly or indirectly in the, directorship, management or operation of a financial institution or other relevant institutions such as a casino;
- the authority to take all necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function in a DNFBP, for example through evaluating a person on the basis of a 'fit and proper' test;
- the authority to verify that financial institutions and DNFBPs apply and enforce measures consistent with this law also to their foreign branches and majority-owned subsidiaries, to the extent permitted by local laws and regulations;

(*continued*)

(*continued*)

- the authority to provide prompt and effective cooperation to agencies that perform similar functions in other States;
- the obligation to maintain statistics concerning measures adopted and sanctions imposed in enforcing AML/CFT requirements; and
- the authority to apply effective, proportionate and dissuasive regulatory or supervisory sanctions for failure by accountable persons to comply with their AML/CFT obligations.

(2) *The supervisory authority shall issue [insert directions/regulations/guidelines] to assist accountable persons to implement their AML/CFT obligations under this Act. An accountable person failing to comply with any direction or regulation issued by a relevant supervisory authority shall be liable to an administrative sanction as may be prescribed in the relevant directive or regulation.*

Section 24 Administrative Sanctions

A supervisory authority under Section 23 that discovers a failure by an accountable person it supervises to comply with the provisions of this Part may impose one or more of the measures available to it for administrative violations; and may ban the accountable person [*permanently/for a maximum period of* [*indicate period*]] from pursuing the business or profession that provided the opportunity for the violation to occur.

Drafting note: Supervisory sanctions form the heart of any comprehensive, dissuasive and effective sanctions regime to deal with non-compliance by accountable persons with their AML/CFT obligations.

The measures available could include a written warning, an order to comply with specific instructions (possibly accompanied with a daily fine for non-compliance), a requirement for regular reports on measures undertaken, an administrative fine in an amount sufficient to be effective and dissuasive, an order barring an individual from employment within a sector, a restriction on certain powers of a manager, director or controlling owner, or a requirement for the replacement of such person, the imposition of a conservatorship or the suspension or withdrawal of a licence. Such administrative sanctions are typically found in sector-specific laws or regulations and applied by supervisory authorities.

Section 24 of the model legislative provisions makes such sanctions and measures available to competent supervisory authorities also for violations of or a failure by an accountable person to comply with its AML/CFT obligations, and regardless of whether or not the accountable person acted intentional, recklessly or simply based on a mistake. Jurisdictions should review the administrative

(*continued*)

(*continued*)

sanctions available to their supervisory authorities to ensure that these sanctions include all the measures cited above.

If the measures currently available are not sufficient, Section 24 could be redrafted to list the specific supervisory measures, rather than to refer to existing administrative sanctions.

Section 25 Failure to Comply with Identification Requirements

Any accountable person, including any director, partner, officer, principal or employee thereof, who intentionally:

(1) fails to carry out the a risk assessment pursuant to Section 4; or

(2) fails to undertake the identification of customers or otherwise to fulfil the customer identification or other requirements in accordance with section 5 (2)–(5); or

(3) opens an anonymous account or an account in a fictitious name for a customer in violation of Section 5(1); or

(4) fails to fulfil the obligations relating to the obtaining of information for and processing of a wire transfer as required by Section 14;

(5) establishes a shell bank or enters into a correspondent relationship with a shell bank or a financial institution that allows its accounts to be used by a shell bank;

(6) fails to maintain books and records as required by Section 10; destroys or removes such records; or fails to make such information available in a timely manner in response to a lawful request for such books or records; commits an offence that shall be punishable by imprisonment for up to [insert imprisonment range] or a fine [insert monetary range] or both.

Drafting note: FATF Recommendation *35* provides that there should be 'effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative' in the case of a failure to comply with AML/CFT requirements.

Individuals as well as institutions may engage in conduct that violates the preventive measures mandates in various ways, with differing degrees of seriousness. States should carefully evaluate the range and kinds of sanctions for each failure to comply. As indicated above, administrative sanctions by supervisory authorities are at the heart of any comprehensive sanctions regime for violation of preventive measures by an accountable person. In cases where an accountable person has violated the provisions of the law either intentionally or in a serious, repetitive and/or systematic manner, additional criminal sanctions may be appropriate and useful. Sections 25–30 provide draft language for establishing

(*continued*)

(*continued*)

criminal liability for accountable persons for certain intentional violations of preventive measure provisions.

Drafting authorities should carefully consider the extent to which criminal liability for violation of preventive measures is admissible and desirable in the national context, and remove or amend the language in Sections 25–30 accordingly. Statutory sanctions for criminal offences shall be proportionate to the violation and be neither too harsh nor too lenient. Drafting authorities should note that the sanction provided for within the European regulatory model is for no more than two years' imprisonment for breach of these types of preventive measures.

Section 26 Failure to Fulfil Due Diligence Obligations or Maintain Internal Controls

Any accountable person, including any director, partner, officer, principal or employee thereof, who intentionally:

(1) fails to conduct ongoing due diligence with respect to customers, accounts and transactions in compliance with Section 12;

(2) fails to comply with the obligations for enhanced due diligence in Section 13; or

(3) fails to maintain internal control programmes in compliance with Section 11 or commits an offence that shall be punishable by imprisonment of [insert imprisonment range] or a fine [insert monetary range], or both.

Section 27 Failure in Regard to Suspicious Transaction or Other Reporting

Any accountable person, including any director, partner, officer, principal or employee thereof, who intentionally fails to submit a report to [insert name of FIU] as required by Section 17(1) or provide information as required under Section 17(2) [*add, if appropriate, optional currency transaction reporting section*] commits an offence that shall be punishable by imprisonment of up to [insert imprisonment range] or a fine of up to [insert monetary range], or both.

Section 28 False or Misleading Statements

Any accountable person, including any director, partner, officer, principal or employee thereof, who intentionally makes a false or misleading statement, provides false or misleading information or otherwise fails to state a material fact in connection with his or her obligations under this Part, including the obligation to make a suspicious transaction [***option:*** *or currency transaction*] report, commits an offence that shall be punishable by imprisonment up to [insert imprisonment range] or a fine up to [insert monetary range], or both.

Section 29 Confidentiality Violation

Any accountable person, including any director, partner, officer, principal or employee thereof, who intentionally discloses to a customer or a third party information in violation of Section 20(1) commits an offence under this Part that shall be punishable by imprisonment up to [insert imprisonment range] or a fine up to [insert monetary range], or both.

Section 30 Other Sanctions

An accountable person, including any director, partner, officer, principal or employee thereof, found guilty of any offence in Sections 25–29:

(1) is subject, in addition to the penalties set out therein, to the sanctions and measures available to the competent supervisory, regulatory or disciplinary authority for administrative violations; and

(2) may also be banned [*permanently/for a maximum period of* [*indicate period*]] from pursuing the business or profession that provided the opportunity for the offence to be committed.