Standard 2.4

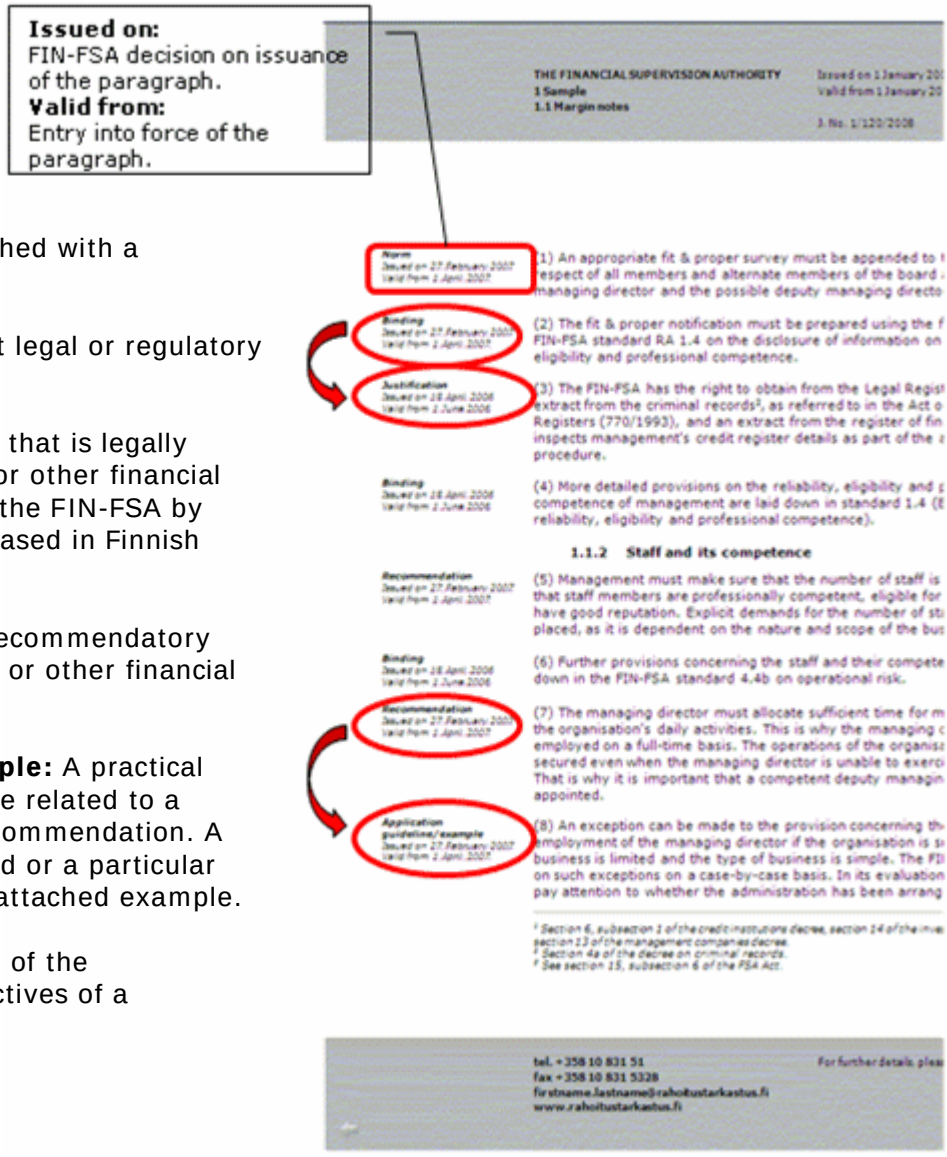
Customer due diligence - Prevention of money laundering, terrorist financing and market abuse

Regulations and guidelines

FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

How to read a standard

A standard is a collection of subject-specific regulations and guidelines which both obliges and guides supervised entities and other financial market participants, indicates the quality level expected by the supervisor, sets out the supervisor's key principles of good practice and provides justification for regulation.



Each paragraph in a standard is furnished with a particular margin note:

- **Norm:** A reference to a current legal or regulatory provision.
- **Binding:** A FIN-FSA regulation that is legally binding on supervised entities or other financial market participants, issued by the FIN-FSA by virtue of its regulatory power based in Finnish law.
- **Recommendation:** FIN-FSA recommendatory guidance to supervised entities or other financial market participants.
- **Application guideline / example:** A practical application guideline or example related to a norm, binding regulation or recommendation. A reference to a FIN-FSA standard or a particular point in the standard. See the attached example.
- **Justifications:** An explanation of the background, purpose and objectives of a regulation or standard.

Sample standard only

FIN-FSA standards may be accessed from www.fin-fsa.fi/eng

TABLE OF CONTENTS

1 APPLICATION

Issued on 23.8.2010
Valid from: 1.9.2010

(1) Chapters 1-5 apply to the following entities and natural persons:

1. credit institutions and financial institutions within the credit institutions' consolidation groups
2. investment firms and financial institutions within the investment firms' consolidation groups
3. fund management companies and custodians
4. the central securities depository
5. book entry registrars
6. payment institutions
7. insurance companies
8. local mutual insurance associations
9. authorised pension insurance companies
10. insurance intermediaries
11. persons referred to in section 7 of the Payment Institutions Act and
12. Finnish branches of foreign credit institutions, investment firms, fund management companies, payment institutions and insurance companies.

Issued on 23.8.2010
Valid from: 1.9.2010

(2) In chapter 5 on customer due diligence, the paragraphs marked as binding are the Financial Supervisory Authority's (FIN-FSA) binding regulations for the entities listed on bullet lines 1–6 in paragraph (1) above. The binding paragraphs on risk management (15, 19, 50, 51, 52, 57, 71, 86, 89, 92, 95, 104 and 115) in chapter 5 also obligate the entities on bullet lines 7–8 in paragraph (1). The application guidelines provided by FIN-FSA in this standard apply to the entities on bullet lines 9–12. In addition, FIN-FSA recommends that the entities on bullet lines 9–12 arrange their operations according to the paragraphs marked as binding in chapter 5.

Issued on 22.6.2010
Valid from: 1.9.2010

(3) Chapters 1–4 and chapter 6 on the reporting obligation concerning suspicious securities trading and other suspect transactions shall be applied to

the following securities intermediaries as referred to in chapter 1, section 4 of the Securities Markets Act (495/1989):

1. credit institutions providing investment services
2. investment firms
3. fund management companies providing investment services (portfolio management)
4. Finnish branches of foreign investment firms
5. Finnish branches of foreign credit or financial institutions providing investment services
6. Finnish branches of foreign fund management companies providing investment services.

Issued on 22.6.2010
Valid from: 1.9.2010

(4) In this standard the generic term *supervised entity* refers to all entities and natural persons in paragraph (1) above, unless otherwise specified. Chapter 6 only applies to securities intermediaries, which are generally referred to in this standard as *parties subject to the reporting obligation*.

Issued on 22.6.2010
Valid from: 1.9.2010

(5) Below, the concept of preventing and detecting money laundering also covers preventing and detecting terrorist financing, unless otherwise specified.

Issued on 22.6.2010
Valid from: 1.9.2010

(6) The Finnish branches of foreign entities listed in paragraph (1) above shall comply with the host country's (Finland) provisions on customer due diligence and preventing and detecting money laundering and terrorist financing. FIN-FSA is not empowered to issue binding regulations for foreign branches in Finland, so in their case the standard is applicable as a recommendation.

Issued on 22.6.2010
Valid from: 1.9.2010

(7) The Finnish branches of foreign entities listed in paragraph (3) above shall comply with the host country's (Finland) provisions on reporting of suspicious securities trading and other suspect transactions. FIN-FSA is also empowered to issue regulations for foreign branches in Finland on the contents and procedure of such reporting.

Issued on 22.6.2010
Valid from: 1.9.2010

(8) Foreign providers of cross-border financial, insurance and payment services without a place of business in Finland are not subject to the Finnish provisions on preventing and detecting money laundering and terrorist financing or the reporting obligation concerning suspicious securities trading and other suspect transactions, but must observe the regulation of their home countries. In problem situations, these providers of cross-border services may contact the Finnish National Bureau of Investigation's Financial Intelligence Unit or FIN-FSA.

Issued on 22.6.2009
Valid from: 1.9.2010

(9) All entities supervised by FIN-FSA must comply with the Act on Preventing and Detecting Money Laundering. The supervised entities may employ

practical solutions applicable to their own operations in performing their duties and risk management concerning customer due diligence and preventing and detecting money laundering and terrorist financing. The functions of the supervised entities within the scope of application differ regarding, among other things, the scope of operations, the entity's organisation and customer structure, the nature of services and the distribution channels.

Issued on 22.6.2010
Valid from: 1.9.2010

(10) A separate FIN-FSA reporting standard RA2.1 has been issued on the contents and procedure governing the reporting of suspicious securities trading and other suspect transactions.

2 OBJECTIVES AND STRUCTURE

Issued on 22.6.2010
Valid from: 1.9.2010

(1) The objective of chapters 1–5 is to provide regulations and guidelines for entities supervised by FIN-FSA to comply with the provisions on customer due diligence and preventing and detecting money laundering and terrorist financing.

Issued on 22.6.2010
Valid from: 1.9.2010

(2) Chapter 5 deals with the key obligations of customer due diligence and risk management in customer relationships. With this standard, FIN-FSA aims to provide regulations and guidelines on arranging risk management in supervised entities' customer relationships and compliance with a diligent and uniform code of conduct in the financial market.

Issued on 22.6.2010
Valid from: 1.9.2010

(3) However, the standard does not contain detailed regulations and guidelines on all obligations under the regulation of the subject area, so the supervised entities shall also have internal instructions applicable to their own operations. According to FIN-FSA, initiatives pursued by organisations representing supervised entities for the purpose of enhancing a uniform code of conduct among their members deserve to be supported.

Issued on 22.6.2010
Valid from: 1.9.2010

(4) FIN-FSA has a legal obligation to monitor that supervised entities comply with their obligations as provided in the Act on Preventing and Detecting Money Laundering. FIN-FSA aims to work in cooperation with other domestic and international authorities and to actively keep abreast of international developments in the subject area.

Issued on 22.6.2010
Valid from: 1.9.2010

(5) In line with the provisions on market abuse and cooperation between authorities supervising the securities markets, chapter 6 of this standard and the related reporting standard RA2.1 provide more detailed instructions on reporting suspicious securities trading and other suspect transactions to FIN-FSA. By improving the provisions on preventing market abuse and harmonising supervisory procedures, the supervisors aim to enhance confidence in the securities markets.

3 INTERNATIONAL FRAMEWORK

Issued on 22.6.2010
Valid from: 1.9.2010

(1) Among other documentation, the following recommendations have been taken into account in preparing chapter 5:

Financial Action Task Force on Money Laundering (FATF):
- The Forty Recommendations (2003)
- Special Recommendations on Terrorist Financing (2004)
- Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, High Level Principles and Procedures (2007)
- Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, High Level Principles for the Life Insurance Sector (2009)

Basel Banking Committee on Banking Supervision (BCBS):
- Customer due diligence for banks (2001)
- Consolidated Know-Your-Customer Risk Management (2003)

International Organisation of Securities Commissions (IOSCO):
- Principles on Client Identification and Beneficial Ownership for the Securities Industry (2004)
- Anti-Money Laundering Guidelines for Collective Investment Schemes (2005)

International Association of Insurance Supervisors:
- Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism (2004)

Wolfsberg Anti-Money Laundering Principles:
- Guidance on a Risk Based Approach for Managing Money Laundering Risks (2006)
- AML Principles for Correspondent Banking (2002)
- Statement on AML Screening, Monitoring and Searching (2009)

Issued on 22.6.2010
Valid from: 1.9.2010

(2) In preparing chapter 6, a guideline by the Committee of European Securities Regulators on the application of the Market Abuse Directive has been taken into account. The basic principle of the guideline is that a uniform reporting procedure improves the exposure of abuse:

> The Committee of European Securities Regulators (CESR): Market Abuse Directive, Level 3 – first set of CESR guidance and information on the common operation of the Directive, CESR/04-505b.

4 LEGAL BASIS

4.1 EU legislation

Issued on 22.6.2010
Valid from 1.9.2010

Chapter 5
(1) National legislation on customer due diligence and preventing and detecting money laundering and terrorist financing is based on the following directives and regulations:

- Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (32005L0060; OJ L 309/15, 25.11.2005) (below the Anti-Money Laundering Directive)
- Commission Directive 2006/70/EC laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of "politically exposed person" and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of financial activity conducted on an occasional or very limited basis (32006L0070; OJ L 214/29, 4.8.2006) (below the Commission's Implementing Directive)
- Regulation (EC) No 1781/2006 of the European Parliament and of the Council on information on the payer accompanying transfers of funds (32006R1781; OJ L 345/1, 8.12.2006) (below the Payer Information Regulation).

Issued on 22.6.2010
Valid from 1.9.2010

Chapter 6
(2) National legislation on the reporting obligation concerning suspicious securities trading and other suspect transactions is based on the following directives:

- Directive 2003/6/EC of the European Parliament and of the Council

on insider dealing and market manipulation (market abuse) (32003L0006; OJ L 96, 12.4.2003)

- Commission Directive 2004/72/EC implementing Directive 2003/6/EC of the European Parliament and of the Council as regards accepted market practices, the definition of inside information in relation to derivatives on commodities, the drawing up of lists of insiders, the notification of managers' transactions and the notification of suspicious transactions (32004L0072; OJ L 162, 30.4.2004, articles 7–11).

4.2 Finnish legislation

Issued on 22.6.2010
Valid from 1.9.2010

(3) The key national legislation on customer due diligence (chapter 5) comprises:

- the Act on Preventing and Detecting Money Laundering and Terrorist Financing (503/2008, below the Anti-Money Laundering Act or AMLA)
- the Government Decree on Preventing and Detecting Money Laundering and Terrorist Financing (616/2008, below the Anti-Money Laundering Decree or AMLD)
- the Ministry of the Interior Decision on non-EEA states and territories whose provisions on preventing and detecting money laundering and terrorist financing meet the requirements laid down in the Act on Preventing and Detecting Money Laundering and Terrorist Financing (78/2009)
- the Government Decision on states and territories whose provisions on preventing and detecting money laundering and terrorist financing do not comply with the international requirements laid down in the Act on Preventing and Detecting Money Laundering and Terrorist Financing (492/2010, below the GovD)
- section 145 of the Credit Institutions Act (121/2007, below the CIA)
- section 69 of the Investment Firms Act (922/2007, below the IFA)
- section 144 of the Mutual Funds Act (48/1999, below the MFA)
- section 29 b of the Act on the Book Entry System (826/1991, below the BESA)
- section 39 of the Payment Institutions Act (297/2010)
- section 16 of the Ministry of Finance Decree on the information to be appended to the authorisation application of a credit institution (939/2007)

- section 12 of the Ministry of Finance Decree on the information to be appended to the authorisation application of an investment firm (937/2007)
- section 12 of the Ministry of Finance Decree on the information to be appended to the authorisation application of a fund management company or custodian (938/2007)
- chapter 32, sections 6–10 (on money laundering offences) of the Criminal Code (39/1889, below the CC)
- chapter 34 a, section 5 (on terrorist financing) of the Criminal Code
- chapter 46, sections 1–3 (on regulation offences, regarding financial sanctions, for example) of the Criminal Code
- section 19, subsection 2, point 7 and section 30 of the Credit Information Act (527/2007)
- the Act on Strong Electronic Identification and Electronic Signatures (617/2009, below the Identification Act) and
- the Personal Data Act (523/1999).

Issued on 22.6.2010
Valid from 1.9.2010

(4) The national legislation on the reporting obligation concerning suspicious securities trading and other suspect transactions (chapter 6) comprises:

- chapters 5 and 10 of the Securities Markets Act (495/1989) and
- chapter 51 of the Criminal Code (39/1889).

4.3 FIN-FSA regulation

Chapter 5

Issued on 22.6.2010
Valid from 1.9.2010

(5) FIN-FSA's power to issue regulations on the code of conduct in customer due diligence and on risk management in preventing and detecting money laundering and terrorist financing are based on the following provisions:

- section 145 of the Credit Institutions Act
- chapter 6, section 10, point 3 of the Insurance Companies Act (521/2008, below the ICA)
- section 69 of the Investment Firms Act
- section 144 of the Mutual Funds Act
- section 29 b of the Act on the Book Entry System
- chapter 10, section 4 a of the Local Mutual Insurance Associations Act (1250/1987)
- section 39 of the Payment Institutions Act (297/2010).

Chapter 6

Issued on 22.6.2010
Valid from 1.9.2010

(6) FIN-FSA's right to issue regulations on the reporting of suspicious securities trading and other suspect transactions (reporting procedure and

contents) are based on the following provisions:

- chapter 4, section 16 and chapter 10, sections 1, 1 a and 1 b of the Securities Markets Act (495/1989)
- chapter 2, section 6 d of the Act on the Operation of a Foreign Credit Institution or Financial Institution in Finland (1608/1993)
- chapter 2, section 4 c of the Act on the Right of a Foreign Investment Firm to Provide Investment Services in Finland (580/1996).

5 CUSTOMER DUE DILIGENCE

5.1 General principles

Justification
Issued on 22.6.2010
Valid from : 1.9.2010

(1) Customer due diligence (CDD) is a key obligation of the Anti-Money Laundering Act. It means that supervised entities identify and know their customers and the nature and extent of customers' business. Customer due diligence refers to all procedures by which supervised entities assure themselves of customers' true identity and of the fact that they know the customers' activities and background to such an extent as required by the nature of the customer relationship. The AMLA requires that supervised entities assess the adequacy of these procedures on the basis of risk analyses.

Application guideline
Issued on 22.6.2010
Valid from : 1.9.2010

(2) The main rule is that supervised entities should not have unidentified (anonymous) customers.[1] Supervised entities have the right to refuse customers that do not give information on themselves or their operations or whose size, place of business or nature of operations is in conflict with the business strategy of the entity. If, for example, a customer relationship or order represents an increased risk of money laundering or terrorist financing, the supervised entity need not establish the relationship or perform the transaction. However, legislation defines certain services[2] that supervised entities can refuse to provide only for strong reasons. For example, one strong reason is that the supervised entity cannot reliably identify the customer.

Application guideline
Issued on 22.6.2010
Valid from : 1.9.2010

(3) Supervised entities should have adequate risk management systems for assessing risk exposures to customers in their activities.[3] Due diligence procedures and risk management for prevention of fraud, such as money laundering, need not be organised in a unit separated from the rest of the risk management or business operations. Thus the unit may be integrated with the supervised entity's general risk management and internal control.

[1] *See section 6, subsection 2 and section 7, subsection 1 of the AMLA.*
[2] *See section134 of the CIA and section 10, subsection 4 of the BESA.*
[3] *See section 6, subsection 3 of the AMLA.*

Application guideline/example
Issued on 22.6.2010
Valid from : 1.9.2010

(4) A risk-based approach to customer due diligence means that supervised entities adjust their customer due diligence measures to the services offered to customers and the money laundering and terrorist financing risks.[4] Supervised entities should employ enhanced due diligence to such customer relationships, transactions and services where they assess increased risk of abuse to be involved, such as money laundering or terrorist financing risks. In customer relationships where supervised entities, on good grounds, have calculated with only minor or no money laundering and/or terrorist financing risks, normal due diligence is sufficient. In certain situations, the AMLA allows simplified customer due diligence.

Application guideline
Issued on 22.6.2010
Valid from: 1.9.2010

(5) The elements of customer due diligence are:[5]

- customer and customer representative identification
- customer identity verification
- identity verification of customer representatives, if necessary
- beneficial owner identification and identity verification, if necessary
- obtaining information on the purpose and nature of business relationships (obtaining information on customer relationships)
- data documentation and period of retention of records
- risk-based ongoing monitoring of transactions and customer relationships
- compliance with the obligation to obtain information when unusual or suspicious transactions are detected.

5.1.1 Risk-based approach

Application guideline
Issued on: 22.6.2010
Valid from: 1.9.2010

(6) A risk-based approach[6] means that supervised entities create customer due diligence procedures adjusted to their own operations and risks and adequate risk management procedures to prevent abuse, money laundering and terrorist financing. For this purpose supervised entities should go through their internal processes in order to assess money laundering and terrorist financing risks related to their customers, products, services, distribution channels and the technological developments and prepare practises for risk mitigation.

[4] *See section 6, subsections 3–5 of the AMLA.*
[5] *See chapter 2 of the AMLA.*
[6] *See section 6, subsections 3–4 of the AMLA.*

Justification
Issued on 22.6.2010
Valid from 1.9.2010

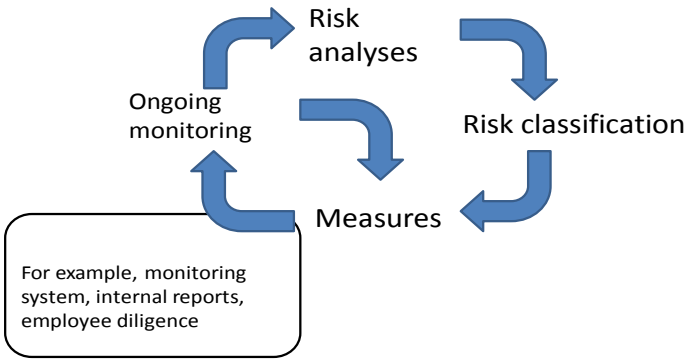
(7) The purpose of developing the risk management procedures is to enable supervised entities to

- identify the risks related to their own customers, products and services
- regularly assess the suitability and appropriateness of the risk management procedures and practices applied
- create customer due diligence procedures concerning different customers, prepare internal instructions applicable to their own operations and train their employees to follow the instructions
- organise their operations in a reliable manner (internal control, monitoring and reporting)
- keep up ongoing and risk-based monitoring of customer relationships and services.

Application guideline/example
Issued on 22.6.2010
Valid fro : 1.9.2010

(8) The picture below shows as an example how a supervised entity's procedures for risk management and ongoing monitoring may affect its operations. Customer due diligence procedures and ongoing monitoring can be adapted variously to different customer groups, products and services on the basis of the supervised entity's own risk assessments and decisions.

Risk-based assessment (example application of section 6, subsection 3 of the AMLA)



Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(9) Due diligence procedures can be divided into normal procedures, simplified procedures and enhanced procedures.[7]

[7] *See section 6 of the AMLA.*

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(10) Normal procedures mean that the supervised entity has decided on a minimum level to be applied in customer due diligence, that is in its measures to ensure customer due diligence in its daily operations. On the basis of risk-based assessment, the supervised entity also detects the customer groups, services or products representing increased risks, where it should apply more extensive customer due diligence procedures (enhanced procedures). Correspondingly the supervised entity can apply normal or simplified procedures to low-risk customer and business relationships and products.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(11) Sections 17–20 of the AMLA provide examples of situations that require enhanced due diligence procedures. Naturally, supervised entities can also apply enhanced procedures to other customer relationships or services according to their own risk assessments or decisions. (See section 5.5 below.)

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(12) Supervised entities may apply simplified customer due diligence procedures only in certain situations as referred to in sections 13–16 of the AMLA. The provisions in force do not allow supervised entities to apply simplified procedures more extensively at their own discretion. (See section 5.6 below.)

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(13) Here is a list of typical situations and cases to be taken into account in risk surveys:

a) Customer characteristics

- Establishing a customer relationship with a politically exposed person requires special procedures for customer approval and enhanced customer due diligence.[8]
- If the customer is a Finnish authority, the supervised entity may apply simplified due diligence.[9]
- In the case of ordinary natural persons, the supervised entity may as a rule apply normal customer due diligence.[10]
- If a legal persons´ ownership or activities are arranged through a complicated structure, sufficient due diligence generally requires that information on both beneficial owners and direct owners is obtained and that the monitoring is more frequent than normally.[11]
- When the customer operates in a business sector observed to be connected to the grey economy or carries out its business in a way that gives the supervised entity reason to suspect that it acts as a straw man for criminal activity, customer due diligence

[8] *See section 20 of the AMLA and section 1 of the AMLD.*
[9] *See section 13 of the AMLA.*
[10] *See sections 6–7 of the AMLA.*
[11] *See sections 6 and 8 of the AMLA.*

requires gathering of sufficient information and ongoing monitoring of the customer relationship.[12]

b) Country and counterparty risk

- Establishing a correspondent bank or comparable relationship requires obtaining sufficient information on the credit or financial institution acting as counterparty, approval by upper management or some other relevant party and ongoing monitoring of the business relationship.[13]
- Such foreign payments whose target country or country of origin is subject to financial sanctions or whose legislation on prevention of money laundering and terrorist financing does not meet with international standards according to the relevant Government Decision[14] require both monitoring of payments and enhanced customer due diligence (for example, trade finance services).[15]

c) Agents and outsourced activities

- The supervised entities are also responsible for their agents' activities and for outsourced services. The arrangement of customer due diligence procedures shall be clearly specified in agreements between the supervised entity and the supplier of services and in the instructions of both parties.[16]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(14) The risk assessments must be updated regularly, taking into account any changes occurring in the services provided by the supervised entity and/or the activities of the customer (for example, introduction of new products, system changes and changes in customer ownership structure and business activities). According to section 6, subsection 5 of the AMLA, the supervised entities shall be able to demonstrate to FIN-FSA that their customer due diligence and risk management procedures are sufficient in relation to the existing risks and that the money laundering and terrorist financing risks related to the entity's nature of operations, customer relationships, products, services and to technical developments have been assessed.

[12] *See sections 6 and 8 of the AMLA.*
[13] *See section 19 of the AMLA.*
[14] *See GovD 492/2010.*
[15] *See section 17 of the AMLA.*
[16] *See standard 1.6 on outsourcing arrangements.*

5.2 Organisation of operations

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(15) The supervised entity's board of directors is responsible for the arrangement of risk management and internal control.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(16) Efficient risk management and internal control involves adoption by the supervised entity of principles for customer due diligence and prevention of abuse, money laundering and terrorist financing. Risk management also includes clear organisation and division of responsibilities in the supervised entity, agreed procedures for different situations and regularly instructed and trained employees.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(17) The board of directors, managing director and other senior management should ensure that agreed principles are consistently observed throughout the consolidation group of the supervised entity, including its foreign subsidiaries and branches.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(18) Credit institutions, financial institutions, investment firms, payment institutions, fund management companies, insurance companies, local mutual insurance associations and insurance intermediaries should ensure that their branches in non-EEA countries, and companies where they hold more than the majority of the voting rights granted by shares and interests, comply with customer due diligence provisions corresponding with the Finnish Anti-Money Laundering Act. If the local legislation prevents compliance with chapter 2 of the AMLA, the supervised entity should so inform FIN-FSA.[17]

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(19) The organisational structure of the supervised entity shall include the appointment of a contact person responsible for the prevention of money laundering and terrorist financing.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(20) The position and duties of the supervised entity's contact person may vary according to the organisational structure of the entity. The contact person must be in an independent, preferably non-business position with the powers and capacity to act in such practical matters related to the prevention of money laundering and terrorist financing as require immediate action, such as reporting suspicious transactions or responding to enquiries from authorities.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(21) The contact information of the contact person should be submitted to the Financial Intelligence Unit combating money laundering.

[17] *See section 21 of the AMLA.*

5.2.1 Internal instructions and training of employees

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(22) As a rule topical legislation and instructions issued by authorities are kept at a general level, and they do not always provide answers to all practical situations pertaining to different customer relationships or services.

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(23) Supervised entities shall have internal instructions on customer due diligence procedures and compliance with the obligation of obtaining information and reporting suspicious transactions to prevent money laundering and terrorist financing. The instructions shall be adapted to their own operations and services.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(24) The instructions should take into account, among other things, internal processes, distribution channels and products as well as outsourced activities and agent relationships. The instructions should also consider product and system developments and expansion of operations into new markets.

Norm
Issued on 22.6.2010
Valid from 1.9.2010

(25) Supervised entities shall see to it that their employees are given proper training in order to ensure compliance with the provisions on preventing money laundering and terrorist financing.[18]

Application guideline/example
Issued on 22.6.2010
Valid from 1.9.2010

(26) Regular, comprehensive training of employees should be arranged at all levels of the organisation, particularly for such groups of employees as are involved in customer relations, product development, clearing, safe-keeping, and payment and/or settlement systems. All training should be recorded in a separate training register.[19]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(27) The obligation of protecting employees as referred to in the AMLA means that the employer should have adequate and appropriate procedures for protecting employees who report suspicious transactions to the Financial Intelligence Unit.[20]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(28) The obligation of protecting employees can be fulfilled through, among other things, instructions and internal training of employees. In addition, supervised entities should take into account the secrecy obligation in section 25 of the AMLA, according to which employees of an entity must not disclose to a customer that a report has been sent. The supervised entity should also see to it that the identities of employees who do such reporting are not disclosed to customers.

[18] *See section 34, subsection 1 of the AMLA.*
[19] *See section 34, subsection 1 of the AMLA.*
[20] *See section 34, subsection 2 of the AMLA.*

5.3 Customer identification and identity verification

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(29) Customer identification and identity verification are key obligations of customer due diligence. Through the identification and verification, the supervised entity ensures that it knows with whom it deals, on whose orders transactions are made and who provides the means. Furthermore, customer due diligence requires that adequate and appropriate information is obtained on the nature and extent of customers' business.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(30) If a supervised entity executes a single transaction of less than EUR 15,000 without establishing a regular customer relationship, it does not, as a rule, need to obtain due diligence information on the customer.[21] However, in transfers of funds, the provisions of the Payer Information Regulation on payer identification and identity verification should be followed.[22]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(31) Customer identification refers to procedures by which supervised entities establish the identity of natural or legal persons based on information provided by the customer or a party aiming for a customer relationship. Identity verification again means ascertaning, the authenticity of personal information obtained in connection with the identification on the basis of documents or information obtained from a reliable and independent source.[23]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(32) The supervised entities are responsible for customer identification, identity verification and customer due diligence also when the identification and due diligence measures are performed by an agent of the entity or some other external party.[24] (See sections 5.3.2–5.3.3 below.)

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(33) Customers should be identified and their identity verified at the beginning of each customer relationship, before any business transactions are conducted. In exceptional cases, customer identification can be finalised at a later stage, but in any case before the customer obtains control over assets or other property involved in a transaction or before the transaction is concluded.[25]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(34) According to the AMLA, a supervised entity has an identification and verification obligation whenever it:[26]

---

[21] *See section 7, subsection 1, point 2 of the AMLA.*
[22] *See articles 4–5 of the Payer Information Regulation.*
[23] *See section 5, subsection 1, points 5–6 of the AMLA.*
[24] *See section 36 b of the CIA, section 30, subsection 2 of the IFA, section 26 a, subsection 7 of the MFA and sections 23–24 of the Payment Institutions Act.*
[25] *See section 7, subsection 4 of the AMLA.*
[26] *See section 7 of the AMLA.*

- establishes a customer relationship with a new customer (regular customer relationship)
- suspects that a previously identified regular customer's identification and verification data are not sufficient or reliable
- without establishing a customer relationship, carries out (with a non-regular customer) a single transaction that individually or as the sum of interrelated transactions amounts to at least EUR 15,000[27]
- detects a suspicious transaction or suspects that funds included in the transaction are being used for terrorist financing or attempting such
- performs a transfer of funds exceeding EUR 1,000, not withdrawn from the customer account (cash payment).[28]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(35) If a supervised entity is not able to identify a customer or perform other customer due diligence measures, it should refuse to establish a customer relationship or perform a transaction. In such case the supervised entity should consider reporting the case to the Financial Intelligence Unit.[29]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(36) A representative acting on behalf of a legal or natural person should be identified and the identity verified, if necessary.[30]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(37) In the event that the guardian of interest of a minor who lacks legal capacity performs a transaction or submits an assignment on behalf of the minor, the minor lacking legal capacity should be identified. However, the minor's identity need not be verified, if the supervised entity, based on a risk assessment, finds verification unnecessary. The person acting as guardian (representative) should always be identified and the identity verified, if necessary.

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(38) The supervised entity shall ensure that the representative is authorised to carry out legal actions on behalf of the customer/principal.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(39) The supervised entity should also identify a beneficial owner and make a risk-based assessment of whether the beneficial owner's identity must be verified.[31]The identity of an insurance contract beneficiary should be verified at the latest when the beneficiary's insurance-based right is to be realised.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(40) In order to be able to identify a beneficial owner, the supervised entity could, in addition to information obtained from the customer, determine the ownership and control structures of any customer that is a legal person.

[27] *The supervised entity may by its own decision set a lower limit.*
[28] *See article 5.4 of the Payer Information Regulation.*
[29] *See section 6, subsection 2 of the AMLA.*
[30] *See section 7, subsection 3 of the AMLA.*
[31] *See section 8, subsection 1 of the AMLA.*

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(41) However, a beneficial owner need not be identified, if the customer is a company or body whose securities have been admitted to public training on regulated markets in one or several EEA member states, as referred to in Directive 2004/39/EC, or if the customer is a company publicly quoted in a third country and subject to disclosure requirements corresponding to Community legislation.[32]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(42) Nor do credit institutions need to identify beneficial owners of pooled accounts held by advocates or other bodies providing legal services in Finland or another EEA member state, provided that the information on the identity of the beneficial owners is available to the credit institutions on request. If an advocate or other body providing legal services operates outside the EEA, the beneficial owners of pooled accounts need not be identified, provided the information on the identity of the beneficial owner is available to the credit institution and the advocate and/or other body providing legal services is subject to obligations corresponding to the Finnish Anti-Money Laundering Act and the party's compliance with these obligations is monitored.[33]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(43) A credit institution need not identify the beneficial owners of pooled accounts related to the performance of duties of attorney.[34]

5.3.1 Identification and verification procedures

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(44) When a customer relationship is established face-to-face with the customer, the identity should be verified on the basis of a valid identification document issued by authorities.[35]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(45) If the customer relationship is established without meeting the customer face-to-face, the supervised entity should have procedures in place for verifying the customer's identity reliably.[36] One verification method is to use electronic identification device fulfilling the criteria of strong electronic identification device or qualified cerficate as referred to in the Identification Act.

Recommendation
Issued on 22.6.2010
Valid from 1.9.2010

(46) In non-face-to-face identifications, identity verification may require a combination of several different methods and gathering additional information from the customer. If necessary, the information provided by the customer should be checked against information available in public registers, such as the Population Information System, Credit Information Register and Trade Register. For reliable customer identification it is not necessarily sufficient that

[32] *See section 8, subsection 2 of the AMLA.*
[33] *See section 8, subsections 3–4 of the AMLA.*
[34] *See section 8, subsection 5 of the AMLA.*
[35] *See section 5, subsection 1, point 5 of the AMLA.*
[36] *See section 18 of the AMLA.*

the supervised entity establishes that the funds have been transferred from an account in the credit institution.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(47) A party that offers the service of strong electronic identification as referred to in the Identification Act should notify the register of the Finnish Communications Regulatory Authority and comply with the authority's regulations.[37] Section 17 of the Identification Act includes provisions on initial identification of an applicant for a strong electronic identification device. The applicant for such an identification device should be identified in person in connection with its first application for identification device as referred to in the Identification Act.

Recommendation
Issued on 22.6.2010
Valid from 1.9.2010

(48) Identification and identity verification of, and delivery of identifier (access codes) to, applicants other than those applying for strong electronic identification device[38] as referred to in the Identification Act should also be performed with due diligence, preferably in person. Alternatively the supervised entity may use registered letters and acknowledgements of receipt, in which case the applicant collects the identifiers from the post office.

Application guideline / example
Issued on 22.6.2010
Valid from 1.9.2010

(49) Here is a list of typical identification and verification procedures for use when establishing a customer relationship:

- Employees of the supervised entity establish the identity of the customer and verify the identity in a face-to-face encounter.
- An agent or other party to whom operations have been outsourced establishes and verifies the customer's identity in a face-to-face encounter.
- A third party establishes and verifies the customer's identity in a face-to-face encounter.[39]
- Neither the supervised entity nor any other party meets the customer face-to-face. Instead the customer identification is based on:
    - a qualified certificate or strong electronic identification device[40] as referred to in the Identification Act
    - identification and identity verification performed by the post office: contracts and/or other documents can be sent as registered mail against acknowledgement of receipt, so that the customer collects the delivery personally. The post office delivers the acknowledgement of receipt to the supervised entity.

---

[37] *See section 10 of the Identification Act and regulations 7b and 8b of the Finnish Communications Regulatory Authority.*
[38] *Here electronic identification refers to, for example, identifiers (access codes) that the customer can only use for internal online services in the institution's financial group.*
[39] *See section 11 of the AMLA.*
[40] *See the Identification Act.*

- In addition, in remote services there is reason to find out, for example, the account numbers of the customer's own bank account and book-entry account and ensure that the transactions are transferred via the accounts indicated in advance by the customer.

5.3.2 Outsourcing and use of agent or third party

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(50) If the customer due diligence procedures are carried out by an agent or outsourced party of the supervised entity, the entity shall ensure that the agent or party to whom the operations are outsourced complies with the entity's instructions on customer identification and due diligence. In contracts covering such services, procedures as well as tasks and responsibilities of both parties shall be agreed on. In addition, the supervised entity shall require that documentation on the customer relationship is submitted to the entity or made available to the entity without delay throughout the customer relationship and the period of retention defined in the AMLA.[41]

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(51) Supervised entities shall provide instructions for and train, as necessary, agents or parties to whom they have outsourced customer due diligence duties.

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(52) The supervisory power and right to obtain information shall remain with FIN-FSA despite the use of an agent or the outsourcing of operations. The outsourcing contract shall include a clause according to which FIN-FSA is entitled to inspect the outsourced operations and obtain information on them.[42]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(53) A third party can also fulfil the customer due diligence obligations on behalf of the supervised entity.[43] A third party is a party with whom the supervised entity does not have an outsourcing or agency agreement. As a rule, the third party is another authorised party subject to the reporting obligation who has corresponding obligations of customer due diligence and prevention of money laundering and terrorist financing. In addition, the operations of a third party must be supervised. For more exact specification of third parties, see section 11, subsections 1–3 of the AMLA.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(54) The supervised entity should ensure that it obtains, from a third party, the information on a customer as referred to in section 10, subsection 2, points 1–8 of the AMLA before carrying out a transaction. In addition, the supervised entity should ensure that all customer due diligence information is

[41] *See section 36 b of the CIA, section 30, subsection 2 of the IFA, section 26 a, subsection 7 of the MFA, sections 23–24 of the Payment Institutions Ac and chapter 6, section 9 and section 10, point 3 of the ICA.*
[42] *See section 36 b of the CIA, section 30, subsection 2 of the IFA, section 26 a, subsection 7 of the MFA, sections 23–24 of the Payment Institutions Ac and chapter 6, section 9 and section 10, point 3 of the ICA.*
[43] *See section 11 of the AMLA.*

available to it and that the third party submits the information on request.

Recommendation
Issued on 22.6.2010
Valid from 1.9.2010

(55) While relying on the due diligence procedure applied by a third party, the supervised entity should be well acquainted with how the third party performs the customer identification and identity verification.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(56) The responsibility for customer due diligence, ongoing monitoring and compliance with the obligation of obtaining and reporting information remains with the supervised entity in all situations.

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(57) The maintenance of customer due diligence information and the ongoing monitoring and compliance with the obligation of obtaining information shall be arranged so that these arrangements do not impair the risk management relating to customer relationships.[44]

5.3.3 Verification documents

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(58) The identity of a natural person should be verified with a document obtained from a reliable and independent source.[45] Verification of identity should be based on a valid official identification document. The reliability of the document should be based on counterfeiting difficulty and a reliable granting procedure.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(59) A natural person should be unambiguously identifiable and the relevant personal information explicitly verifiable from a verification document. The document should contain a photo and be valid for a fixed time. If the supervised entity suspects the authenticity of an identification document presented by a customer or the customer cannot be verified from it, the entity has the right and obligation to require additional proof by the customer for identity verification. If necessary, the supervised entity should supplement and check the identity verification information provided by the customer from public registers.

Application guideline/example
Issued on 22.6.2010
Valid from 1.9.2010

(60) Valid versions of the following documents issued by Finnish authorities are commonly used for identity verification in Finland:

- driving licence[46]
- identification card[47]
- passport[48]
- diplomatic passport[49]

[44] *See standard 1.6 on outsourcing arrangements.*
[45] *See section 5, subsection 1, point 5 of the AMLA.*
[46] *See the Driving Licence Decree (845/1990).*
[47] *See the Identification Card Act (829/1999).*
[48] *See the Passport Act (671/2006).*

- alien's passport and refugee travel documents[50]
- SII card containing photo[51].

Supervised entities may also verify a natural person's identity using valid documents granted by foreign authorities, such as:

- national passport
- identification card acceptable as travel document.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(61) On the basis of its own risk management principles, the supervised entity may decide which of the above-mentioned documents it will accept for verification purposes. As regards verification documents, there is no general national legislation specifying acceptable verification documents. However, in Finland passports and identification cards issued by the police are the only documents issued explicitly for proving a person's identity.

Application example
Issued on 22.6.2010
Valid from 1.9.2010

(62) If a supervised entity accepts a driving licence as a verification document, it should take into account that the process of granting a driving licence is not the equivalent of that for granting a passport or identification card, and that driving licences are deficient in terms of security features.

Application example
Issued on 22.6.2010
Valid from 1.9.2010

(63) The supervised entity should particularly pay attention to replaced driving licences that are used for identity verification. According to international traffic agreements, a foreigner can have his driving licence replaced by a Finnish licence after residing in the country for half a year. Thus a person whose identity the authorities have not been able to confirm and whose travel documents include notice of such can replace his driving licence with a Finnish one that does not include any such notice.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(64) When a supervised entity acts as an identification service provider as referred to in the Identification Act, it should perform the initial identification in person and with due care. An identification service provider should identify an applicant for an identification device by verifying the applicant's identity from a valid passport or identification card for travelling issued by an EEA member state, Switzerland or San Marino. For initial identification purposes, the identification service provider may also use a valid driving license issued by an EEA member state authority after 1 October 1990 or a valid passport issued by a Government authority of another state.[52]

---

[49] *See the Passport Act (671/2006).*
[50] *See chapter 8 of the Aliens Act (301/2004).*
[51] *The Finnish Social Insurance Institution has not issued new SII cards with photo since 13 October, 2008.*
[52] *See section 17, subsection 1 of the Identification Act.*

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(65) Identity verification of a legal person is based on an up-to-date extract from the Trade Register or a corresponding extract from some other official register that establishes the existence and legal capacity of the legal person as well as the members of the board of directors or other decision-making body.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(66) A person representing a legal person should be identified and, if necessary, the identity should be verified (according to a risk-based approach).[53]

Application guideline/example
Issued on 22.6.2010
Valid from 1.9.2010

(67) If necessary, the scope of authority of a legal person's representative should be confirmed via a separate power of attorney or an extract from the minutes of a decision-making body of the legal person.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(68) In general, information on the beneficial owners of a legal person is not provided by the Trade Register or other public registers. In the course of determining who the beneficial owners are, the supervised entity may ask a representative of the legal person for information on the legal person's ownership and group structure and persons with a controlling interest. For example, the information can be obtained from a limited company's list of shareholders, minutes, contracts or other documents on the company's ownership and control structures.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(69) The supervised entity can perform an identity verification of the beneficial owners based on risk-based consideration.[54]

5.4 Obtaining customer due diligence information

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(70) The scope of information to be obtained for customer due diligence can vary. It is affected by the supervised entity's risk assessments of the effects on its operations of different customer relationships and services provided. Obtaining sufficient information on a customer relationship enables detection of unusual transactions during the customer relationship and supports compliance with the obligation of obtaining information and reporting suspicious transactions.

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(71) The supervised entity shall have internal instructions including specification of the information to be obtained on establishing different customer relationships.

[53] *See section 7, subsection 3 of the AMLA.*
[54] *See section 8, subsection 1 of the AMLA.*

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(72) Due diligence information[55] according to the obligations presented in chapter 2 of the AMLA should also, if necessary (according to a risk-based approach), be obtained on customer relationships established prior to 1 August 2008 (when the current AMLA came into force). The due diligence information should be updated systematically.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(73) In addition to identification and contact information, the following information should be obtained from the customer (depending on the customer relationship):[56]

- information on the customer's transactions, nature and extent of the customer's business and grounds for the use of a service or product
- information on the customer's representatives, beneficial owners, ownership structure, financial status and on the source of funds.

The information obtained from the customer can be compared to information received from public registers (for example, the Population Information System, Credit Information Register or Trade Register). The supervised entity can also check the customer's credit information when establishing the customer relationship as part of the customer due diligence procedure.[57]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(74) If a supervised entity, based on its own risk survey or other information available, assesses that a customer's operations represent an undue risk of money laundering or terrorist financing, enhanced procedures should be applied to customer due diligence, which means that additional information on the customer relationship should be obtained and the information and details checked.[58]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(75) In certain situations cited particularly in the AMLA, the supervised entity may on the other hand apply simplified due diligence, or obtain less information on the customer relationship, such as beneficial owners, and refrain from verifying the information.[59]

5.5 Enhanced customer due diligence

Norm
Issued on 22.6.2010
Valid from 1.9.2010

(76) According to section 17 of the AMLA, the supervised entity shall comply with enhanced customer due diligence obligations (extra carefully) in situations where the customer, service, product or transaction represents an increased risk of money laundering or terrorist financing or where the

[55] *See section 46 of the AMLA.*
[56] *See section 10 of the AMLA.*
[57] *See section 19, subsection 2, point 7 of the Credit Information Act (527/2007).*
[58] *See section 17 of the AMLA.*
[59] *See sections 13–16 of the AMLA.*

customer is connected with a state whose system for preventing and detecting money laundering and terrorist financing does not comply with international standards.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(77) The AMLA contains examples of customer relationships requiring enhanced customer due diligence:

- if a customer relationship is established without the customer being physically present, customer identification and identity verification should be performed with enhanced care (non-face-to-face identification, section 18 of the AMLA)
- customer relationship with a politically exposed person or with a family member or a close associate of such a person (PEP customer, section 20 of the AMLA)
- correspondent banking or corresponding business relationship across EEA borders (section 19 of the AMLA)
- on the basis of its own risk assessment, the supervised entity considers that a certain customer relationship, product, distribution channel or transaction requires application of enhanced procedure (section 17 of the AMLA).

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(78) An enhanced due diligence obligation requires extended examination and documentation of the customer's operations and use of services. In ongoing monitoring, particular account should be taken of customer relationships subject to enhanced due diligence.

5.5.1 Customer or transaction connected with certain states

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(79) Supervised entities should comply with enhanced due diligence obligations, if a customer or a customer transaction is connected with a state whose system for preventing and detecting money laundering and terrorist financing does not comply with international standards.[60]

Application guideline/example
Issued on 22.6.2010
Valid from 1.9.2010

(80) FATF has issued statements on countries and jurisdictions whose legislation and systems for prevention of money laundering and terrorist financing do not comply with international standards. Correspondingly, in Finland a Government Decision has been taken regarding states that do not comply with international standards.[61] These states may also be subject to financial sanctions by the EU and UN. The supervised entity should pay particular attention to and apply enhanced due diligence to customers and transactions related to these states.

[60] *See section 17 and section22, subsection 3 of the AMLA.*
[61] *See Government Decision 492/2010 and section 22, subsection 3 of the AMLA.*

Application example
Issued on 22.6.2010
Valid from 1.9.2010

(81) A connection as referred to in section 17 of the AMLA could exist, if, for example, one party of a transaction is from a state that does not comply with international standards against money laundering and terrorist financing, if the registered office of a legal person is in such a state or if a customer deals in products subject to international sanctions, such as import or export restrictions. Enhanced obligations may also be necessary, if a payment included in a transaction is paid from or to an account in a credit institution located in a state as referred to above.

Application guideline/example
Issued on 22.6.2010
Valid from 1.9.2010

(82) In addition, the supervised entity should comply with an enhanced reporting obligation, if a customer or transaction is connected with a state whose system of preventing and detecting money laundering and terrorist financing does not comply with international standards.[62] A report should be sent to the Financial Intelligence Unit, if

- the customer does not provide the requested details to enable the supervised entity to fulfil its obligation to obtain information
- the supervised entity considers the provided information unreliable
- the basis or origin of the transaction is not sufficiently accounted for
- the legal person cannot be identified or
- the beneficial owner or person on behalf of whom the customer is acting cannot be identified or established in a reliable manner.

5.5.2 Non-face-to-face identification

Norm
Issued on 22.6.2010
Valid from 1.9.2010

(83) If the customer is not physically present for identification and identity verification (non-face-to-face identification, section 18 of the AMLA), the party subject to the reporting obligation shall take the following measures to mitigate the risk of money laundering and terrorist financing:

1. verify the customer's identity on the basis of additional documents or information obtained from a reliable source
2. ensure that the payment of the transaction is made from the credit institution's account or to an account that was opened earlier in the customer's name or
3. verify the customer's identity by means of a qualified certificate, as referred to in the Identification Act, or some other electronic identification that ensures information security and is verifiable.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(84) Supervised entities should have a procedure for checking information that the customer has given via non-face-to-face identification. A supervised entity may require that the customer submits additional documentation and details, thus verifying the provided information (see section 5.3.2 on identification and verification procedures and section 5.4 on obtaining

[62] *See section 24 of the AMLA.*

customer due diligence information).

5.5.3 Correspondent banking or corresponding business relationship

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(85) The correspondent banking relationship in section 19 of the AMLA refers to a contract that a credit institution concludes with another credit institution located in a non-EEA state. The purpose of such a business relationship is, for example, to transfer payments, provide clearing and settlement services and execute other orders between the credit institutions. A correspondent banking relationship is comparable with a corresponding business relationship that an insurance company, investment firm, fund management company or payment institution has established with a party operating outside the EEA.

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(86) Supervised entities shall have internal instructions on obtaining sufficient information and documentation on the counterparty, on internal decision-making powers and procedures and on enhanced due diligence procedures required in correspondent banking or corresponding business relationships.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(87) Prior to establishing a business relationship, the supervised entity should obtain sufficient information on the correspondent bank or a credit institution, investment firm, fund management company, insurance company or payment institution that is the counterparty in a corresponding contract. In particular, information should be obtained on the counterparty's authorisation, the supervision it is subject to and whether it applies (in its own customer relationships) at least a similar regulation to prevent money laundering and terrorist financing as the supervised entity itself applies. The supervised entity should form a well-founded opinion of the counterparty's reputation and nature of business. The customer due diligence obligations to be fulfilled should be agreed on in a contract. Establishing a business relationship requires approval by upper management. The business relationship should be monitored on a regular basis.

Application guideline / example
Issued on 22.6.2010
Valid from 1.9.2010

(88) From a risk management viewpoint, it may be useful to the supervised entity to obtain information on the counterparty's financial position, customers and business sector. Such information can be obtained from the counterparty itself or from public registers.[63]

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(89) Adequate risk management requires that the supervised entity ensures that a counterparty correspondent bank does not allow shell banks to use its accounts.[64]

[63] *For example, the Banker's Almanac database.*
[64] *See article 14.5 of the Money Laundering Directive.*

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(90) Supervised entities should be especially vigilant, if a correspondent bank or the counterparty in a corresponding business relationship operates in a state whose system for preventing and detecting money laundering and terrorist financing does not comply with international standards or if the counterparty is included in the public warning lists of, for example, FATF or foreign supervisors. If the counterparty is subject to financial sanctions by the UN or EU, this could, depending on the contents of the sanction, mean that the supervised entity should not establish or maintain a correspondent banking or corresponding business relationship with such a counterparty.

5.5.4 Business relationship with a shell bank

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(91) A shell bank is a financial institution or company who typically

- has been authorised in a state known as a "tax haven"
- does not carry out financial activities in the state where it is authorised
- does not have a place of business in any state
- is not subject to public supervision
- does not provide information on its owners or beneficial owners or
- does not provide reliable information on its activities or financial position.

Shell banks' activities may be related to financial crime, such as tax evasion or money laundering. A business relationship with a shell bank represents an exceptional exposure to money laundering or terrorist financing.

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(92) Entities supervised by FIN-FSA must not enter into or maintain business relationships with shell banks.[65]

5.5.5 Politically exposed persons

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(93) Persons are considered politically exposed[66], if, during the course of the past twelve months, they have acted as another state's

- Head of State, Head of Government, minister, deputy or assistant minister
- Member of Parliament
- member of supreme court, member of constitutional court or member of some corresponding judicial body whose decisions are not generally subject to further appeal
- member of court of auditors or of the highest decision-making body of an authority auditing the management of Government funds and corresponding to the State Audit Office
- member of the Board of the central bank

[65] *See article 13.5 of the Money Laundering Directive and page 24 of Government Bill 25/2008.*
[66] *See section 20 of the AMLA and section 1 of the AMLD.*

- ambassador or chargé d'affaires
- high-ranking officer in the armed forces
- member of the administrative, management or supervisory body of a state-owned company.

The following are categorised as family members of politically exposed persons as listed above:

- spouse or partner considered equivalent to spouse
- children and their spouses or partners
- parents.

Close associates of politically exposed persons are those specified in the Anti-Money Laundering Decree (section 1, subsection 3 of the AMLD).

Application guideline/example
Issued on 22.6.2010
Valid from 1.9.2010

(94) Politically exposed persons also comprise another state's Members of the EU Parliament, commissioners and Members of the EU Court of Justice or EU Court of Auditors. In Finland, corresponding Finnish EU officials are not considered politically exposed persons.

Application guideline/example
Issued on 22.6.2010
Valid from 1.9.2010

(95) Supervised entities shall create procedures and internal instructions for establishing and maintaining customer relationships with politically exposed persons, their family members and close associates.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(96) Prior to establishing the customer relationship, the customer should be approved by upper management. The supervised entity should examine the origin of property and assets related to the customer relationship or transaction in question. The established business relationship should be subject to enhanced monitoring.[67]

5.6 Simplified customer due diligence

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(97) In situations described in sections 13–16 of the AMLA, supervised entities may apply simplified customer due diligence. Simplified customer due diligence is sufficient for the low-risk insurance products listed in the Act, that is low-risk from a money laundering and terrorist financing point of view, and for certain legal persons and authorities about which there is public and reliable information available.[68]

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(98) Application of section 12 of the AMLA requires that the Government issues a decree with more detailed information on customers, products, transactions and services representing a low money laundering and terrorist

[67] *See section 20, subsection 2 of the AMLA.*
[68] *See article 3.1 of the Commission's Implementing Directive.*

financing risk.[69] As long as no such decree has been issued, the supervised entity cannot apply a simplified customer due diligence procedure at its own discretion as referred to in section 12.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(99) A simplified customer due diligence procedure may be applied (according to the following exhaustive list)[70], if the customer is

- a Finnish authority or a comparable party, such as a municipality, the Social Insurance Institution or the Bank of Finland
- a credit institution, insurance company, financial institution, investment firm, fund management company or payment institution that is duly authorised in an EEA state
- a credit institution, insurance company, financial institution, investment firm or fund management company duly authorised in a non-EEA state and subject to obligations equivalent to those laid down in the Finnish Anti-Money Laundering Act and supervised for compliance with these obligations
- a branch located in an EEA state of a credit institution, insurance company, financial institution, investment firm or fund management company duly authorised in a non-EEA state
- a company whose securities are admitted to public trading according to the Securities Markets Act and who is subject to disclosure requirements similar to those in the Markets in Financial Instruments Directive.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(100) A simplified customer due diligence procedure may be applied to the following insurance products specified in the AMLA (according to the following exhaustive list):[71]

- an insurance policy the periodic premium of which does not exceed EUR 1,000 or single premium of which does not exceed EUR 2,500
- a statutory employee pension insurance policy or a pension insurance policy of a self-employed person which does not include a surrender clause and cannot be used as collateral
- a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made via deductions from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(101) A simplified customer due diligence procedure may be applied to electronic money, if the electronic device cannot be recharged and the electronic money stored therein does not exceed EUR 150 or, correspondingly,

[69] *See section 22, subsection 2 of the AMLA.*
[70] *See sections 13–14 of the AMLA.*
[71] *See section 15 of the AMLA.*

the device can be recharged but the recharge amount in the same calendar year is at most EUR 1,000.[72]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(102) The simplified procedure does not release the supervised entity from its customer due diligence obligations.[73] The supervised entity should obtain sufficient information on the customer to be able to ensure that the customer or product is one of those referred to in paragraphs 99–101 above and to detect unusual patterns in the customer operations. In fact, the simplified procedure requires that the supervised entity at least identifies its customer (and customer representative, if necessary). Based on a risk-based assessment, the supervised entity may simplify its due diligence procedure by, for example, refraining from finding out about or verifying beneficial owners or the ownership structure.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(103) Nor does the simplified procedure release the supervised entity from its ongoing monitoring arrangements.[74] The supervised entity should be able to detect, among other things, such changes in the customer's environment or operations that would render the customer unsuitable for simplified due diligence.

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(104) Supervised entities shall have internal instructions for complying with the simplified procedure.

5.7 Documentation and retention of identification records

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(105) Section 10 of the AMLA contains provisions on retention of records and sections 23 and 25 provisions on retention, handling and secrecy of information necessary to comply with the obligation of obtaining information and reporting suspicious transactions. The AMLA also contains provisions on sanctions against violating the obligation to keep records (section 40 of the AMLA).

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(106) Personal data necessary for compliance with the customer due diligence obligations should be handled according to section 8, subsection 1, point 4 of the Personal Data Act. Appropriate retention, processing, secrecy and protection of personal data should be carefully planned and performed.[75] Customers' personal data should regularly be updated.[76]

[72] *See section 16 of the AMLA.*
[73] *See section 12 of the AMLA.*
[74] *See section 12 of the AMLA.*
[75] *See section 5 of the Personal Data Act.*
[76] *See section 9 of the Personal Data Act.*

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(107) According to the AMLA, supervised entities should also update the information on customer relationships established prior to 1 August 2008 to make it compatible with the current customer due diligence obligations.[77] The updating can be performed according to the supervised entity's risk-based assessment and flexibly in connection with, for example, meetings with the customers or when new customer contracts are concluded.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(108) Customer identification and due diligence should be documented and the information retained for five years after termination of a regular customer relationship. In the case of an occasional transaction exceeding EUR 15,000, the period of retention is five years after execution of the transaction.[78] Otherwise, transaction information and documents should be retained according to, among other things, the Accounting Act.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(109) Identification, identity verification and customer due diligence information should be documented and retained so that the supervised entity can later show the authorities how each customer was identified, which documents or what information was used as proof of identity and who carried out the customer identification. In addition, for customer due diligence and risk management of the customer relationship, the supervised entity should retain sufficient and essential information on the customer, its representatives, ownership structure and beneficial owners as well as members of a legal person's board of directors or corresponding decision-making body. The retention duty also applies to information on the nature of customer activities, the legal person's ordinary industry sector, the scope of operations and the services provided by the supervised entity and the use thereof.[79]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(110) The details and information obtained to comply with the reporting obligation as referred to in the AMLA (sections 23–24) should be retained separately from the customer identification, verification and due diligence information.[80] Such information includes, for example, the detailed information obtained by the supervised entity when considering reporting to the Financial Intelligence Unit combating money laundering.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(111) A customer has access to its own due diligence information registered by the supervised entity. Because a report on suspicious transactions may not be revealed to the customer, it does not have access to the information obtained to comply with the obligation of obtaining information and reporting suspicious transactions.[81] Also findings detected as a result of ongoing monitoring can be classified as risk management information, to which the

[77] *See section 46 of the AMLA.*
[78] *See section 10, subsection 1 of the AMLA.*
[79] *See section 10 of the AMLA.*
[80] *See section 23, subsection 4 of the AMLA.*
[81] *See section 23, subsection 5 of the AMLA.*

customer does not have access.

5.8 Ongoing monitoring arrangements

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(112) Ongoing monitoring refers to procedures by which the supervised entity monitors customer relationships and use of services to ensure that the customer operations are consistent with the entity's experience and knowledge of the customers and their business.

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(113) The purpose of ongoing monitoring is to develop customer due diligence and risk management in customer relationships. Another purpose is to support detection of unusual use of services and prevent and reveal abuse and criminal activities, such as money laundering and terrorist financing.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(114) Supervised entities should arrange adequate monitoring in light of the nature, extent and risks of customer operations.[82]

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(115) The ongoing monitoring shall be systematic and comprehensive considering the scope of operations and the risks in customer relationships. The supervised entity shall have internal instructions for using ongoing monitoring procedures as well as adequate resources and internal control.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(116) Supervised entities' operations differ from each other and thus the needs and procedures of ongoing monitoring can vary. The procedures can be both automatic solutions and manual methods and their combinations. Using different methods, the monitoring can focus on transactions, payments and customer relationships. The vigilance and professional skills of employees are still key factors in detecting unusual transactions, but systemic monitoring supports the manual monitoring.

Application example
Issued on 22.6.2010
Valid from 1.9.2010

(117) The monitoring can be based on reports prepared by the supervised entity for other risk management. For example, it can be implemented as part of normal monitoring and reporting of customers and services. Systemic monitoring can be implemented by using different scenarios and parameters for selecting transactions from, for example, outgoing and incoming payments found to be unusual on the basis of size, structure or frequency. Sufficient resources should be allocated to analysing unusual transactions.

[82] *See section 9, subsection 2 of the AMLA.*

5.8.1 Payer Information Regulation

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(118) The purpose of the Payer Information Regulation is to ensure that authorities can trace transfers of funds related to criminal activities and particularly money laundering and terrorist financing. The regulation aims to ensure sufficient information on the original payer in cross-border payments in order to reduce anonymous payments and payments with missing information on the payer. The regulation is directly applicable legislation in all EU member states.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(119) The regulation applies to payments in all currencies. The regulation should not be applied to direct debiting nor to check or debit card payments. Cash payments to the payer's own account and cash payments through accounts are also considered transfers of funds as referred to in the regulation. Thus cash payment customers must be identified for retention and communication of the payer information. In cash payments exceeding EUR 1,000, the identity of the payer must also be verified.[83]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(120) The payment service provider of the payer is responsible for seeing that outgoing transfers of funds include the payer information required in the regulation:[84]

- Payments from or to non-EU states should include complete information on the payer: payer name, address and account number. Instead of the address, the payer's date and place of birth, customer identification number or national identity number can be provided. If the payer has no account number, it can be replaced by an individual code by which the transfer of funds can be traced back to the payer.
- Internal EU payments can be compared with domestic payments; they should include the payer's account number or an individual code by which the transfer of funds can be traced back to the payer. However, the payment service provider of the payer should also provide complete information with internal EU payments, if the payment service provider of the payee requires such information.[85]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(121) The information included with the payment should be retained throughout the payment chain, and the intermediary payment service provider may not remove the information. The payment service provider of the payee should monitor incoming payments to be able to detect payments

[83] *See articles 3.1–2 and 5 of the Payer Information Regulation.*
[84] *See article 5.1 of the Payer Information Regulation.*
[85] *See article 6 of the Payer Information Regulation.*

with missing or obviously false information on the payer.[86]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(122) When the payment service provider of the payee detects payments with missing or false information, it should either ask for the missing information from the payment service provider of the payer or reject the payment. However, the payment may be executed, if the information is not so incomplete that the supervised entity rejects or suspends the payment according to its own procedure. If deficiencies in incoming payments are recurrent and frequent, the supervised entity should complain to the payment service provider of the payer. If, despite complaints, the deficiencies are not corrected, the supervised entity may issue a warning, terminatethe correspondent banking relationship or report the payment service provider to FIN-FSA.[87] If the payment is unusual or suspicious, the supervised entity should report it to the Financial Intelligence Unit.[88]

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(123) Supervised entities providing payment services shall have in place procedures and methods for ongoing monitoring of both outgoing and incoming payments. In addition, payment service providers shall provide internal instructions and methods for possible rejection of incoming payments.

5.8.2 International financial sanctions

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(124) The international sanctions binding Finland are imposed by the UN Security Council and European Council. The sanctions are implemented through EU regulations, which are directly applicable legislation in all EU member states. The sanctions are a means of bringing pressure to bear in the international security policy and they are used for regulating restrictive measures pertaining to certain states, groups or persons. Another purpose of the sanctions is to prevent terrorist activities and financing. There are various forms of sanctions including, for example, export and import sanctions and financial sanctions. The names of individuals, entities, groups or other parties subject to sanctions are published as appendices to the regulations.

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(125) The purpose of financial sanctions is to freeze such funds and other financial resources as are owned, held or controlled by governments, individual government members, other controlling parties or leaders of armed groups that are subject to sanctions. In addition, sanctions may include a prohibition against financing such parties or a prohibition against directly or indirectly releasing or transferring funds to parties subject to sanctions. Also banks and their foreign branches and private persons may be subject to

[86] *See article 8 of the Payer Information Regulation.*
[87] *See article 9.2 of the Payer Information Regulation.*
[88] *See article 10 of the Payer Information Regulation.*

financial sanctions.

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(126) Finnish enforcement of EU financial sanctions is based on the Sanctions Act.[89] The right of processing personal information necessary for compliance with sanctions is based on section 8, subsection 1, point 4 of the Personal Data Act.[90] Financial sanctions oblige supervised entities to freeze the funds of individuals, organisations and entities as referred to in regulations without a separate decision by the authorities. Failure to comply with the obligations should be punished as a regulation offence under chapter 46 of the Criminal Code.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(127) Supervised entities should follow changes in financial sanctions and regularly check their registers and monitor payments and other transactions to ensure that they do not provide services or transfer payments to parties subject to financial sanctions. It is prohibited to release or transfer funds or, in certain cases, other financial resources, to such parties directly and indirectly. Account should be taken of the sanctions in the supervised entity's management of country risks, correspondent banking relationships, financial services for import and export businesses and product-related processes. Customer relationships or transactions having a connection with states that are subject to financial sanctions require enhanced due diligence.[91]

Application guideline/example
Issued on 22.6.2010
Valid from 1.9.2010

(128) In the event that a supervised entity finds in its files or registers a person with identification details matching those of a party subject to sanctions, it must freeze the assets and notify the Financial Intelligence Unit and the Ministry of Foreign Affairs. If a supervised entity finds a person with identification details similar (close match) to those of a party subject to sanctions, the entity need not freeze the assets, but it should notify the Financial Intelligence Unit and act according to the unit's instructions (for example, the identification details in the list of parties subject to sanctions may be incomplete, thus making it impossible for the supervised entity to ensure on its own that the detected party is identical with the listed party).

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(129) In addition to UN and EU sanctions, several states and authorities have imposed their own national sanctions. These sanctions are not legally binding in Finland. The most well known of such sanctions are those of the US Office of Foreign Assets Control (OFAC), which lists persons and entities whose

[89] *See the Act on the Enforcement of Certain Obligations of Finland as a Member of the United Nations and of the European Union (659/1967, the Sanctions Act).*
[90] *See section 8, subsection 1 of the Personal Data Act: "Personal data shall be processed only if: 4) processing is based on the provisions of an Act or it is necessary for compliance with a task or obligation to which the controller is bound by virtue of an Act or an order issued on the basis of an Act."*
[91] *See GovD 423/2010 and section 17 of the AMLA.*

assets should be frozen according to OFAC.[92] The OFAC lists are published on the authority's own website.

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(130) Financial institutions should ensure that their customers are not among the listed parties, that these parties are offered no services and that no payments are transferred for them. US banks also freeze payments to listed parties from sources outside the USA. It is also possible that intermediary banks in the payment chain freeze such payments. On the basis of the USA Patriot Act, US authorities may also impose sanctions on foreign financial institutions that do not comply with OFAC sanctions.

Recommendation
Issued on 22.6.2010
Valid from 1.9.2010

(131) Although the OFAC sanctions lists are not legally binding in Finland and supervised entities thus not obliged to freeze assets in Finland of parties included in those lists, the monitoring of OFAC lists can, on good grounds, be considered to fall within the obligation to obtain information as referred to in section 9, subsection 3 of the AMLA. Suspending transactions for further enquiries can also be justified as compliance with section 26, subsection 1 of the AMLA. Because US banks are obliged to freeze payments connected with OFAC-listed parties, supervised entities should take account of this fact in their own risk management.

5.9 Compliance with the obligation of obtaining information and reporting suspicious transactions

Justification
Issued on 23.8.2010
Valid from 1.9.2010

(132) Compliance with the obligation to obtain information as referred to in the AMLA requires that supervised entities have adequate knowledge of their customers' activities so that they can detect unusual orders or transactions and report them. Having detected an unusual transaction, a supervised entity should fulfil the obligation of obtaining information as referred to in section 9, subsection 3 of the AMLA and, if necessary, the reporting obligation as referred to in section 23, subsection 1 of the AMLA. Supervised entities that fail to comply with the obligation to obtain information or report suspicious transactions may run the risk of sanctions under AMLA.[93]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(133) The reporting obligation can also arise on the basis of the EU Payer Information Regulation, the enhanced due diligence obligation according to the AMLA or international financial sanctions.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(134) Supervised entities should detect and examine unusual orders or transactions in the financial market. Supervised entities should consider reporting orders or transactions that are unusual in the following ways as

[92] *See the list of Specially Designated Nationals and Blocked Persons.*
[93] *See sections 40 and 42 of the AMLA.*

described in the AMLA:[94]

- their structure or size deviate from the ordinary
- they deviate from the ordinary in relation to the supervised entity's size or place of business
- they do not have a clear financial purpose
- they are in conflict with the customer's financial standing or other business activities.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(135) Having detected an unusual transaction, a supervised entity is obliged, within reasonable means available, to examine the background of the transaction as well as the origin and purpose of funds included. Information may be obtained from, for example, official registers or the supervised entities' own registers or by requesting more detailed information on the transaction from the customer, such as contracts or other documents supporting the transaction. Supervised entities are also entitled to check customers' credit information.[95]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(136) Supervised entities should act without delay so that funds or other assets related to a suspicious transaction are not transferred beyond authority access. If their suspicions are aroused, supervised entities may, at their own discretion, take the following courses of action:[96]

- suspension of a transaction for enquiries[97]
- rejection of a transaction, if, for example, the customer's identity cannot be reliably established
- execution of a transaction, if the supervised entity cannot leave the transaction unexecuted or suspension or rejection of the transaction is likely to hinder discovery of the beneficiary of the transaction.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(137) Supervised entities should inform the Financial Intelligence Unit, if

- a transaction is suspicious even after enquiries have been made[98] to fulfil the obligation to obtain information (section 9, subsection 3 of the AMLA)
- a customer is unwilling to provide the requested information
- the supervised entity considers the provided information unreliable
- the supervised entity rejects the execution of a suspicious transaction
- the supervised entity executes a suspicious transaction (section 26 of the AMLA)

---

[94] *See section 9, subsection 3 of the AMLA.*
[95] *See section 19, subsection 7 of the Credit Information Act.*
[96] *See section 26 of the AMLA.*
[97] *The AMLA obligation imposed on supervised entities to suspend a suspicious transaction for further enquiries (section 26, subsection 1 of the AMLA) overrules, among other things, provisions on payment transfer.*
[98] *See section 23, subsection 1 of the AMLA.*

- the supervised entity, after execution of the transaction, obtains information that renders the transaction suspicious.

Justification
Issued on 22.6.2010
Valid from 1.9.2010

(138) When a suspicious transaction is reported to the Financial Intelligence Unit, the report is not a report of an offence (investigation request). It is a report based on a supervised entity's detection of an unusual transaction or order in the financial market. No minimum amount (in money) has been specified for such a report. The supervised entity need not know or evaluate what kind of criminal offence may have been committed.

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(139) As a rule, suspicions are reported electronically in accordance with the provisions of the Anti-Money Laundering Decree and detailed instructions of the Financial Intelligence Unit on the contents of the report and the reporting procedure.[99] The report should be prepared so as to enable the Financial Intelligence Unit to evaluate the course of events and the actions taken by the supervised entity. The Financial Intelligence Unit is entitled to obtain from the involved supervised entities[100] all necessary information related to the report and to suspend a transaction for a period of five days.[101]

Application guideline
Issued on 23.8.2010
Valid from 1.9.2010

(140) Supervised entities may be held liable for damages arising from a report only if they have failed to apply such due diligence as, in the circumstances, can reasonably be required.[102] The filing of a report must not be revealed to the reported customer nor to any other person.[103]

Application guideline
Issued on 23.8.2010
Valid from 1.9.2010

(141) Under the conditions laid down in section 25 of the AMLA, the fact that a report has been filed may be revealed to:

- entities as referred to in the Act on the Supervision of Financial and Insurance Conglomerates (699/2004) that belong to the same financial and insurance conglomerate and are authorised in an EEA state
- entities as referred to in the Act on the Supervison of Financial and Insurance Conglomerates that belong to the same financial and insurance conglomerate and are authorised in a non-EEA state, if such entities are subject to obligations corresponding with the Finnish Anti-Money Laundering Act and their compliance with these obligations is monitored
- credit institutons, investment firms, fund management companies and their branches and payment institutions authorised in an EEA state, if they participate in an occasional transaction related to the customer and transaction reported
- credit institutions, investment firms, fund management companies and their branches authorised in a non-EEA state, if the receiver of the

[99] *See section 23, subsection 2 of the AMLA and section 2 of the AMLD.*
[100] *See section 23, subsection 3 of the AMLA.*
[101] *See section 26, subsection 3 of the AMLA.*
[102] *See section 39, subsection 1 of the AMLA.*
[103] *See section 25, subsection 1 of the AMLA.*

revealed information participate in an occasional transaction related to the customer and transaction reported and if it is subject to obligations corresponding with the Finnish Anti-Money Laundering Act and its compliance with these obligations is monitored and the receiver of the information further is subject to personal data protection obligations corresponding with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

When such information is provided, the customer's name, date of birth and personal identity code, the citizenship of a foreign customer and the grounds for making the report may be disclosed. The information received may only be used for preventing money laundering and terrorist financing and it must be retained separately from the customer information. The customer is not entitled to access such information.[104]

[104] *See section 23, subsections 4–5 of the AMLA.*

6 REPORTING OBLIGATION CONCERNING SUSPICIOUS SECURITIES TRADING AND OTHER SUSPECT TRANSACTIONS

Norm
Issued on 22.6.2010
Valid from 1.9.2010

(1) If parties subject to the reporting obligation have reason to suspect that a transaction may involve abuse of inside information or price distortion of a security, as defined in chapter 5 of the Securities Markets Act or chapter 51 of the Finnish Criminal Code, they must report their suspicions to FIN-FSA without delay.[105] (See the separate reporting standard RA2.1.)

Norm
Issued on 22.6.2010
Valid from 1.9.2010

(2) The filing of a report must not be revealed to the suspected party nor to any other persons.[106]

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(3) The Securities Markets Act may oblige parties subject to the reporting obligation to report suspicious securities trading or other suspect transactions. The Securities Markets Act provides that suspicious securities trading and other suspect transactions should be reported to FIN-FSA. Such a report is not a report of an offence (investigation request). Rather it refers to an unusual securities transaction or another irregular transaction (for example, a derivatives transaction), detected by the party subject to the reporting obligation, or to a situation where that party otherwise has reason to suspect unlawful use of inside information or price distortion of a security, in connection with securities trading or another transaction. There is no minimum amount, based on the size of the trade or other transaction, for when a report must be filed. Failure to report may result in administrative sanctions as referred to in the Act on the Financial Supervisory Authority imposed on parties subject to the reporting obligation.

[105] *See chapter 4, section 16, subsection 1 of the Securities Markets Act.*
[106] *See chapter 4, section 16, subsection 2 of the Securities Markets Act.*

Application guideline
Issued on 22.6.2010
Valid from 1.9.2010

(4) The filing of a report may not be revealed to the reported persons nor to their legal or other representatives, as this can jeopardise the investigation of the matter. The extent to which parties subject to the reporting obligation may be held liable for damages is laid down in chapter 4, section 17 of the Securities Markets Act.

7 REPORTING TO FIN-FSA

Binding
Issued on 22.6.2010
Valid from 1.9.2010

(1) A separate FIN-FSA standard RA2.1 has been issued on the reporting of suspicious securities trading and other suspect transactions.

tel +358 10 831 51

firstname.lastname@finanssivalvonta.fi
www.finanssivalvonta.fi

For further details, please contact
Market and Operational Risk, tel. +358 10 831 5207
Markets, tel. +358 10 831 5372

8 DEFINITIONS

Issued on 22.6.2010
Valid from 1.9.2010

(1) Securities trading or other transactions refer to securities trades and other acquisition or disposal of securities (for example, entering into loan agreements or subscribing for shares). Other transactions also refer to derivatives contracts and to the execution of rights and obligations based on derivatives contracts.

Issued on 22.6.2010
Valid from 1.9.2010

(2) Customers refer to natural or legal persons to whom supervised entities offer services or who request or use services provided by supervised entities. Generally the customer is the party in whose name the service or product is recorded in the systems of the supervised entity. Customers can be regular or non-regular customers (occasional customers).

Issued on 22.6.2010
Valid from 1.9.2010

(3) Customer due diligence (CDD) refers to all procedures by which supervised entities assure themselves of a customer's true identity and of the fact that they know the customer's background and activities to the extent required by the customer relationship. Measures related to the customer due diligence obligation should include customer identification and identity verification, identification and, if necessary, verification of representatives and beneficial owners, obtaining information on the nature and extent of business relationships and ongoing monitoring of business relationships.

Issued on 22.6.2010
Valid from 1.9.2010

(4) Customer identification refers to establishment of the identity of a customer or person acting on behalf of the customer on the basis of the information provided by the customer. The identification is one element of the customer due diligence.

Issued on 22.6.2010
Valid from 1.9.2010

(5) Customer identity verification refers to ensuring the customer's identity on the basis of documents, data or information obtained from a reliable and independent source.

Issued on 22.6.2010
Valid from 1.9.2010

(6) Initial identification has been defined in the Act on Strong Electronic Identification and Electronic Signatures (the Identification Act), where section 17 contains provisions on the identification and identity verification of

applicants for a strong electronic identification device.

Issued on 22.6.2010
Valid from 1.9.2010

(7) A suspicious transaction or trade deviates from a typical transaction or trade of the field in terms of, for example, size, structure, size of customer or place of business. The supervised entity need not recognise the characteristics listed in the Criminal Code or know whether the transaction is connected to criminal activity. Supervised entities should fulfil the obligation of obtaining information and reporting suspicious transactions.

Issued on 22.6.2010
Valid from 1.9.2010

(8) Non-face-to-face identification refers to a situation in which the customer is not physically present for identification and identity verification. Establishing the identity of the customer (identification and verification procedure) requires an enhanced procedure, that is enhanced due diligence.

Issued on 22.6.2010
Valid from 1.9.2010

(9) Reporting obligation: 1. Reporting obligation according to chapter 4, section 16 of the Securities Markets Act refers to securities intermediaries' duty to declare suspicious securities trading or other suspect transactions to FIN-FSA; 2. Reporting obligation according to sections 23–24 of the Anti-Money Laundering Act refers to supervised entities' obligation to report suspicious transactions to the National Bureau of Investigation's Financial Intelligence Unit.

Issued on 22.6.2010
Valid from 1.9.2010

(10) Third party is a party which fulfils the customer due diligence obligations on behalf of the supervised entity according to the conditions provided in section 11 of the Anti-Money Laundering Act.

Issued on 22.6.2010
Valid from 1.9.2010

(11) Non-regular (occasional) customers refer to customers that use the services of the supervised entity on a one-off basis for, for example, a single transfer of funds after cash payment or a single subscription in a share issue.

Issued on 22.6.2010
Valid from 1.9.2010

(12) Other senior management includes persons, in addition to the board of directors and CEO, who actually manage the activities of the supervised entity. For example, the manager of an important business line of the supervised entity may be such a person. Together with the board of directors and the CEO, the members of other senior management constitute the senior management of the supervised entity.

Issued on 22.6.2010
Valid from 1.9.2010

(13) Politically exposed person (PEP) is a person who holds or has held an important public position in another state during the last year. The Government Decree on Preventing and Detecting Money Laundering and Terrorist Financing (616/2008) contains more detailed provisions on public positions that render persons politically exposed. As applicable, also EU-level positions can make persons politically exposed. Family members and close associates of politically exposed persons are also specified in the decree. Establishing and mainintaining customer relationships with such persons

requires application of enchanced customer due diligence by supervised entities.

Issued on 22.6.2010
Valid from 1.9.2010

(14) Money laundering: According to chapter 32, section 6 of the Criminal Code, a person who receives, uses, converts, conveys, transfers or transmits property acquired through an offence, the proceeds of crime or property replacing such property, in order to conceal the illegal origin of such proceeds or property or assist the offender in evading the legal consequences of the offence, can be sentenced for money laundering. A person who effaces or conceals the true nature, origin, location or disposition of, or rights to, property acquired through an offence, the proceeds of an offence or property replacing such property or assists another person in such effacement or concealment can also be sentenced for money laundering.

Issued on 22.6.2010
Valid from 1.9.2010

(15) Obligation to obtain information: When a supervised entity detects an unusual or suspicious transaction, it should fulfil the obligation to obtain information referred to in section 9, subsection 3 of the Anti-Money Laundering Act. Among other things, it includes the obligation to examine the background of an unusual and suspicious transaction as well as the origin and purpose of the associated funds. If the transaction seems suspicious even after enquiries into the matter, an obligation of the supervised entity arises to file a report to the Financial Intelligence Unit.

Issued on 22.6.2010
Valid from 1.9.2010

(16) Terrorist financing is punishable on the basis of chapter 34 a, section 5 of the Criminal Code: A person who directly or indirectly provides or collects funds in order to finance, or is aware that these will finance terrorist acts specified in the Code can be sentenced for terrorist financing. The funds may be legally or illegaly acquired. As regards terrorist financing, the suspicion need not focus on the origin of the funds but may focus on the object financed with the funds.

Issued on 22.6.2010
Valid from 1.9.2010

(17) Beneficial owner refers to a natural person on whose behalf a transaction is being conducted or, if the customer is a legal person, the natural person who controls the customer. According to the Anti-Money Laundering Act, a natural person is considered to control a legal person when it holds more than 25% of the voting rights attached to the shares or interests or has the right to appoint or dismiss the majority of members of the board of directors.

In the case of an insurance policy or contract, a beneficial owner is the person who is the beneficiary of an indemnity.

Issued on 22.6.2010
Valid from 1.9.2010

(18) Regular customer refers to a relationship of a permanent nature, involving a customer that uses the services of the supervised entity on a regular basis or a customer who has at least one contract with or commitment to the supervised entity. A regular customer relationship may also be a

relationship that, when the contact is made, is expected to become permanent. Establishing such a customer relationship may include, for example, opening an account, entering into a credit agreement, subscribing for fund units or entering into an agreement for intermediation of securities or execution or transmission of orders.

Issued on 22.6.2010
Valid from 1.9.2010

(19) Upper management here refers to the management directly above the employees asking for approval.

9 REPEALED STANDARDS AND GUIDELINES

Issued on 22.6.2010
Valid from 1.9.2010

(1) FIN-FSA's standard 2.4 entered into force on 1 September 2005.

Issued on 22.6.2010
Valid from 1.9.2010

(2) This standard repeals the FIN-FSA standard 2.4 on customer identification and customer due diligence, prevention of money laundering, terrorism financing and market abuse valid from 1 September 2005.

Issued on 22.6.2010
Valid from 1.9.2010

(3) The standard repeals section 6.9. in standard 4.4b on management of operational risk in the section Capital Adequacy and Risk Management of the FIN-FSA set of regulations.

Issued on 22.6.2010
Valid from 1.9.2010

(4) The standard also repeals

- section 15.2 on prevention of money laundering and terrorist financing in the set of regulations and guidelines, J. No. 2/002/2008, issued by FIN-FSA (the Insurance Supervision Authority) for domestic insurance companies, authorised pension insurance companies, local mutual insurance associations, insurance holding companies, branches of third country insurance companies and insurance institutions established through an Act
- section 13 on prevention of money laundering and terrorist financing in the set of regulations and guidelines, J. No. 8/002/2007, issued by FIN-FSA (the Insurance Supervision Authority) for insurance intermediaries.

10 REVISION HISTORY

Issued on 23.8.2010
Valid from 1 .9.2010

(1) Standard has been revised on 23 August 2010 as follows:

- 1. Application:
  - List of entities in paragraph (1);
    - transferred persons referred to in section 7 of the Payment Institutions Act transferred to the point 11 and
    - added Finnish branches of foreign payment institutions to the point 12;
  - paragraph (2) corrected accordingly
- 5.9 Compliance with the obligation of obtaining information and reporting suspicious transactions:
    - corrected paragraphs (132), (140) and (141)

tel +358 10 831 51

firstname.lastname@finanssivalvonta.fi
www.finanssivalvonta.fi

For further details, please contact
Market and Operational Risk, tel. +358 10 831 5207
Markets, tel. +358 10 831 5372

11 FURTHER INFORMATION

Please find the necessary contact information in the list of Persons in charge of standards on FIN-FSA's website. For further information, please contact:

- Prudential Supervision: Market and Operatonal Risks Division + 358 10 831 5208
- Market Supervision: Markets Division (Chapter 6) + 358 Markets, tel. +358 10 831 5372