

## **KREDITILSYNET**

Norway

Translation date: July 2004

Translated by Government Authorised Translator Mr. Peter Thomas

*This translation is for information purposes only. Legal authenticity remains with the official Norwegian version as published in Norsk Lovtidend.*

---

## **Circular 9/2004**

15 April 2004

### **Guide to new anti-money laundering legislation**

#### **Introduction**

**A new Money Laundering Act and associated regulations went into force on 1 January 2004. The new legislation *widens* the range of persons and undertakings with a reporting obligation (also called “reporting entities” in this guide) to include state authorised and registered auditors, authorised external accountants, real estate agents and co-operative housing associations that provide real estate agency services, along with securities registers (the Central Securities Depository).**

**Under the new money laundering legislation *all entities with a reporting obligation* are obliged to request proof of identity when a customer relationship is established, to investigate any transaction that appears suspicious and to report the transaction to ØKOKRIM<sup>1</sup> if investigation fails to disprove the suspicion. In order to verify his/her identity, a customer must *appear in person* at the premises of the undertaking that is entering into the agreement with the customer, or (in the case of outsourcing) at the premises of another undertaking with a reporting obligation.**

**The new rules also require banks and finance companies to establish electronic monitoring systems by the end of 2004. The rules continue, update and further develop existing anti-money laundering measures and implement the European Union's Second Money Laundering Directive of 2001, see below.**

This circular circulates information on the anti-money laundering legislation to entities with a reporting obligation that fall within Kredittilsynet's supervisory and administrative ambit. The scope of the legislation's application to reporting entities is detailed under the discussion of section 2 of the regulations below. The new money laundering legislation also encompasses lawyers and dealers in valuable objects. These groups can approach ØKOKRIM, professional associations (for example The Norwegian Bar Association) and relevant supervisory agencies for further guidance. The Ministry of Justice is responsible for the legislation on the legal profession.

---

<sup>1</sup> The National Authority for Investigation and Prosecution of Economic and Environmental Crime.

In Chapter 1 Kredittilsynet provides a general review of the new legislation on measures to combat money laundering and terrorist financing.

This is followed in Chapter 2 by a closer look at individual sections of the new Money Laundering Regulations. Particular emphasis is given to describing and explaining the relationship between the Money Laundering Act and the Money Laundering Regulations.

The new money laundering legislation comprises the Act on measures to combat the laundering of proceeds of crime (No. 41 of 20 June 2003, Money Laundering Act), see annex 1, and Regulations on measures to combat the laundering of proceeds of crime etc., (No. 1487 of 10 December 2003, Money Laundering Regulations), see annex 2. The new legislation supersedes sections 2-1, 2-17 and 2-17a of the Act on Financing Activity and Financial Institutions (No. 40 of 10 June 1988) and Regulations on Customer Identification and Measures to Combat Money Laundering (No. 118 of 7 February 1994).

This circular supersedes Kredittilsynet's circular no. 13/1999. Other superseded circulars on money laundering are: 28/1994, 29/1995, 31/1995, 8/1996, 31/1996, 4/1997, 5/1997 and 28/1998.

The circular is designed to make the money laundering legislation more accessible and to clear up a number of practical issues. However, it is not exhaustive and does not address all aspects of the money laundering legislation.

## Table of contents

### Chapter 1: General review of the new Money Laundering Act and associated regulations

- 1.1 Main content of the money laundering legislation
- 1.2 Why institute rules on measures to combat the laundering of criminal proceeds and terrorist financing?
- 1.3 International rules, standards and recommendations in the anti-money laundering field
- 1.4 Measures to combat terrorist acts and terrorist financing
- 1.5 Who should read this circular?
- 1.6 Penal and administrative sanctions

### Chapter 2: Review of individual sections of the new Money Laundering Regulations

- 2.1 Section 1 Scope of application
- 2.2 Section 2 Establishment of customer relationships
- 2.3 Section 4 Requirements on identity documents etc (physical persons)
- 2.4 Section 5 Cases where the customer is unable to produce identity documents
- 2.5 Section 6 Requirements on identity documents etc (legal persons)
- 2.6 Section 7 Exceptions from the obligation to request proof of identity
  - 2.6.1 Exceptions from the identity verification requirement in respect of certain insurance contracts
- 2.7 Section 8 Verification of identity etc
  - 2.7.1 Situations that call for identity verification
  - 2.7.2 Implementation of identity verification
    - 2.7.2.1 Exceptions where appearing in person would cause the customer major inconvenience
    - 2.7.2.2 Exceptions where personal appearance at the primary undertaking is not practicable
    - 2.7.2.3 Further details on the outsourcing of identity verification
    - 2.7.2.4 Outsourcing in the securities field
    - 2.7.2.5 Outsourcing of identity verification to Norway Post's branch network
    - 2.7.2.6 Practical examples of implementation of identity verification
- 2.8 Recapitulation – identity verification
- 2.9 Section 9 Absence of, or inadequate, proof of identity – refusing the customer
- 2.10 Section 10 Investigation of suspicious transactions
- 2.11 Section 11 Submission of data to ØKOKRIM
- 2.12 Section 12 Electronic monitoring systems
- 2.13 Section 13 Special reporting of transactions associated with countries or areas which have not implemented satisfactory anti-money laundering measures etc.
- 2.14 Section 14 Prohibition of or restrictions on the right of reporting entities to establish customer relationships with or undertake transactions to or from countries which have not implemented satisfactory anti-money laundering measures etc.
- 2.15 Section 15 Requirement as to retention and deletion of data etc.
- 2.16 Section 16 Training of employees etc., of reporting entities

## **Chapter 1: General review of the new Money Laundering Act and associated regulations**

### **1.1 Main content of the money laundering legislation**

The money laundering legislation can be divided into three main themes:

- The obligation of reporting entities to request customers to provide proof of identity when establishing a customer relationship and when carrying out certain transactions, and the obligation of institutions to retain a copy of identity documents along with transaction data.
- The obligation to investigate suspicious transactions, and to report to ØKOKRIM should suspicion not be disproved by investigation.
- The obligation of reporting entities to establish routines, initiate training programmes and nominate a money laundering officer – i.e. senior manager with responsibility for dealing with cases of money laundering and terrorist financing.

### **1.2 Why institute rules on measures to combat the laundering of criminal proceeds and terrorist financing?**

For criminals the overriding aim is to gain maximum benefit from the proceeds of crime. An overriding aim of criminal policy is that crime should not pay. That is why the authorities devote a great deal of attention to preventing the laundering of, and to confiscating, criminal proceeds.

The anti-money laundering legislation is also designed to protect institutions from exploitation by criminals and the potential loss of repute, trust and money.

*”Whereas when credit and financial institutions are used to launder proceeds from criminal activities (hereinafter referred to as 'money laundering'), the soundness and stability of the institution concerned and confidence in the financial system as a whole could be seriously jeopardized, thereby losing the trust of the public;”*

Preamble to Council Directive 91/308/EC

### **1.3 International rules, standards and recommendations in the anti-money laundering field**

Under the EEA agreement Norway is obliged to implement the European Union Directive on prevention of the use of the financial system for the purpose of money laundering in national law. The new money laundering legislation implements the EU's second money laundering Directive adopted on 4 December 2001 (2001/97/EC) amending the first money laundering Directive (91/308/EEC) on prevention of the use of the financial system for the purpose of money laundering.

International coordination is an important aspect of anti-money laundering and anti-terrorist financing measures. Norway contributes through its participation in the Financial Action Task on Money Laundering (FATF). In June 2003 FATF adopted forty revised recommendations on anti-money laundering measures. This followed eight special recommendations on terrorist financing adopted by the FATF in 2001. Visit FATF's website at [www.fatf-gafi.org](http://www.fatf-gafi.org) to view both sets of recommendations. A great deal of other useful information on these themes is also published on this website. Although Norwegian authorities have yet to decide whether the revised FATF recommendations from June 2003 call for changes in the Norwegian money laundering legislation, FATF's general and special recommendations clearly represent very important international standards and recommendations in this field.

The Basel Committee on Banking Supervision has identified flaws in banks' "know your client" routines in many countries. In October 2001 the Committee published a report entitled "Customer due diligence for banks", see the [www.bis.org](http://www.bis.org) website. The report establishes new supervisory standards and provides a basis for banks' routines and practice in regard to the "know your client" principle. The report also has a supervisory purpose and is not limited to combating money laundering through the financial system. Non-existent or inadequate "know your client" routines in banks could expose banks to grave customer and counterparty risk, in particular reputational, legal and operational risk.

As indicated above rules, standards and recommendations in the international anti-money laundering arena have been tightened. This affects both the design and enforcement of the Norwegian anti-money laundering legislation.

#### **1.4 Measures to combat terrorist acts and terrorist financing**

Since terrorist acts and terrorist financing are also included in the scope of the new legislation, such acts are addressed by the obligation to investigate and to report suspicious transactions. The legislation makes several references to offences coming under the Penal Code section 147a or section 147b.

These two provisions of the Penal Code are elaborated on in Proposition to the Odelsting No. 72 (2002-2003) page 10:

*“The International Convention of 9 December 1999 for the Suppression of the Financing of Terrorism (Terrorist Financing Convention) and United Nations Security Council Resolution 1373 have been implemented in Norwegian law by amending act no. 54 of 28 June 2002. The amendments include a new penal provision in the Penal Code section 147a which expressly targets terrorist acts. Certain specified criminal acts are now to be regarded as terrorist acts if executed with the intent mentioned in the act; entering into agreement to commit such acts has also been made a criminal offence. Moreover, a new penal provision has been included in the Penal Code section 147b which addresses terrorist financing. This provision targets the procurement of funds or the*

*furnishing of financial services to terrorists or terrorist networks. New rules on the freezing of assets connected with terrorist activity have also been adopted. These rules empower the prosecuting authority, subject to further conditions, to deprive accused persons of the right to dispose over funds or other assets, first and foremost in order to prevent future criminal acts.”*

## **1.5 Who should read this circular?**

Section 4 of the Money Laundering Act lists entities with a reporting obligation to whom the act applies. The list is reproduced below under section 1 “Scope of application”. Managers and staff in reporting entities who work specifically with transactions, clearing functions and internal controls should have a thorough knowledge of the money laundering legislation. The reporting entity's money laundering officer – cf the Money Laundering Act section 13, third sentence, and the Money Laundering Regulations section 11, first paragraph – has a particular obligation to familiarise him/herself with the legislation. (See section 11 below for further details.) When implementing internal controls, the reporting entity’s management board must satisfy itself that the rules are adhered to, and should therefore be acquainted with the main features of the legislation.

## **1.6 Penal and administrative sanctions**

It should be noted that entities with a reporting obligation who deliberately (against their better judgement) violate or assist in the violation of provisions of the Money Laundering Act and associated regulations are punishable by fines or, in particularly aggravating circumstances, by imprisonment of up to one year, unless the offence attracts a stricter penalty. See section 16 of the Money Laundering Act.

In its capacity as an administrative and supervisory agency, Kredittilsynet can also implement administrative measures. See the Money Laundering Act section 17 “Orders and coercive measures”.

## **Chapter 2: Review of individual sections of the new Money Laundering Regulations**

The sections are commented on in numerical order.

### **2.1 Section 1 Scope of application**

According to Section 1 of the Money Laundering Regulations, the new legislation applies to reporting entities listed in section 4 of the Money Laundering Act. Section 4 first and second paragraph of the act reads as follows:

- 1 *financial institutions,*
- 2 *Norges Bank (Central Bank of Norway),*
- 3 *e-money institutions,*

4 persons and undertakings operating activities consisting of transfer of money or financial claims,  
5 investment firms,  
6 management companies for securities funds,  
7 insurance companies,  
8 pension funds,  
9 postal operators in connection with provision of postal services,  
10 securities registers,  
11 other undertakings whose main activity is subject to items 2 to 12 and 14 of annex I to Directive 2000/12/EC relating to the taking up and pursuit of the business of credit institutions, including the provision of loans, stockbroking, payment transmission, financial leasing, advisory services and other services associated with financial transactions and letting of safe deposit boxes.

*The Act also applies to the following legal and natural persons in the exercise of their professions:*

1 state authorised and registered public accountants,  
2 authorised external accountants,  
3 real estate agents and housing associations that act as real estate agents,  
4 insurance brokers,  
5 project brokers,  
6 currency brokers,  
7 lawyers and other persons who provide independent legal assistance on a professional or regular basis when they assist or act on behalf of clients in planning or carrying out financial transactions or such transactions concerning real property or movable property as are referred to in item 8;  
8 dealers in objects, including auctioneering firms, commission agents and the like, in connection with cash transactions of NOK 40 000 or more or a corresponding amount in foreign currency. This shall only apply to transactions involving payment cards when so provided in regulations laid down by the Ministry;  
9 persons and undertakings that, in return for remuneration, offer services corresponding to those referred to in items 1 to 8.

**Further details in relation to securities registers (the Central Securities Depository) – Money Laundering Act section 4, first paragraph, no. 10**

According to section 4 first paragraph no. 10 of the Money Laundering Act, the legislation applies in cases where securities registers themselves opt to act as account operator. The legislation also applies in cases where a securities register utilises another account operator who is not subject to the money laundering legislation. In such cases either the register itself or another account operator has to verify customer identity as required by law and regulations. The Securities Register Act states that the securities register itself is responsible for establishing rules for the use of external account operators, and that such rules have to be approved by Kredittilsynet, cf the Securities Register Act section 1-2. Hence rules governing identity verification etc have to be drawn up either in conformity with the Money Laundering Regulations or with corresponding home-state rules duly approved by Kredittilsynet, before account operators who are not

subject to the money laundering legislation can be utilised. See the Money Laundering Act section 4, third paragraph, which states that “*the act also applies to undertakings and persons who perform services on behalf of or for entities with a reporting obligation*”.

**Further details in relation to undertakings listed in the annex to the Consolidated Banking Directive – Money Laundering Act section 4 first paragraph no. 11**

According to the Money Laundering Act section 4 first paragraph no. 11, undertakings whose main activity is subject to items 2 to 12 and 14 of annex I to the Consolidated Banking Directive (Council Directive 2000/12/EC of 20 March 2000) are encompassed by the money laundering legislation. A copy of the Directive accompanies this circular. One example of such activity is that of undertakings exclusively engaged in foreign exchange activity in conformity with chapter 4a “Foreign Exchange Activity” of the Act on Financing Activity and Financial Institutions (No. 10 of 10 June 1988).

**Application of the money laundering legislation to branches**

Section 3, first paragraph, of the Money Laundering Act states that the act applies to branches of foreign undertakings established in Norway. Pertinent examples are branches of banks and other credit institutions headquartered in another state in the European Economic Area (EEA), cf section 7 in Regulations no. 326 of 2 May 1994 on branches of banks and other credit institutions with their head office in another state in the European Economic Area etc.

**Outsourcing etc.**

According to the Money Laundering Act section 4, third paragraph, the money laundering legislation also applies to “*undertakings and persons who perform services on behalf of or for undertakings and persons with a reporting obligation*”. Hence reporting entities are bound by the money ordering legislation in respect of all forms of outsourcing of licensable activity and all use of agents and independent distributors. See 2.7.2.3 below for further details. The money laundering legislation also applies to any use made of substitutes and all types of temporary labour.

**Debt collection companies and regulated markets**

Section 4 last paragraph of the Money Laundering Act provides for the adoption of regulations making the money laundering legislation applicable to debt collection companies and regulated markets. No such regulations had been adopted by the time this circular was distributed.

**2.2 Section 2 Establishment of customer relationships**

This section states when a customer relationship is considered to be established under the money laundering legislation.

The section refers to the Money Laundering Act section 5 (verification of identity) whose first paragraph, first sentence, states that “*persons or undertakings with a reporting obligation shall upon establishment of a customer relationship request that the customer show valid proof of identity.*” When it establishes a customer relationship, a reporting

entity also incurs several other obligations that are regulated in the money laundering legislation. The main content of these obligations is explained in 1.1 of this circular.

Section 2, first paragraph, of the Money Laundering Regulations states that a customer relationship is considered to be established “*once the customer is able to utilise the services of an entity with a reporting obligation (...)*”. Kredittilsynet interprets this provision to mean that the customer relationship is considered to be established at the earliest point in time at which the customer is able to make use of the reporting entity's services. Hence the reporting entity cannot postpone verification of the customer's identity until, for example, the first payment is made into the account or the first time the customer uses a payment card etc.

Section 2, second paragraph, of the Money Laundering Regulations gives two examples of the point at which a customer relationship is established: “*(...)in connection with the opening of an account or the issue of a payment card.*”

The time at which a customer relationship is established must be concretely assessed for each service offered by the reporting entity. In the following Kredittilsynet gives guidance on the point at which a customer relationship is considered to be established, and at which the requirement as to identity verification comes into play, in the case of some services.

- In the case of **deposit accounts** this point will be upon “*the opening of an account*” – i.e. when the account agreement is entered into. Entities with a reporting obligation cannot wait until the first transaction (crediting, debiting, card use) is carried out before verifying the customer's identity.
- Where **sales finance** – for example of motor vehicles – is concerned, identity verification has to be carried out, at the latest, when the customer actually takes possession of the capital item in question. In such cases the dealer or supplier is empowered to check the customer's identity documents on behalf of the financial institution, cf section 8, second paragraph, of the Money Laundering Regulations and section 4, second, paragraph, no. 8, of the Money Laundering Act (outsourcing).
- Where **payment and credit cards** are concerned, two types are reviewed here:
  - Where the customer applies for current account credit, accessed by card, the customer's identity has to be verified by his/her appearing in person at the premises of the dealer or supplier at the time the account credit agreement is entered into. Alternatively the identity check can be carried out via the customer's personal receipt of the card by registered mail (see 2.7.2.5 below).
  - Where the customer applies for a card which is not related to a concrete purchase of a product or service, the customer's identity has to be verified via the customer's personal receipt of the card by registered mail. If the card is a

"company card", or a card which is issued to the customer based on the latter's employment contract or the like, verification can be carried out by the company, organisation etc guaranteeing the customer's identity. A condition for such an arrangement is that the legal person in question who guarantees the customer's identity has established his identity in accordance with section 6 of the Money Laundering Act.

- Where **subscription of financial instruments** is concerned, identity has to be verified before the transfer of any securities to the customer's Central Securities Depository account takes place and before the customer makes any payment. Hence identity verification must take place no later than when the decision is made to allot securities to the customer. In cases where the institution is also required to open a Central Securities Depository account for the customer, the customer's identity must be verified when the account is established, see section 1 above and the reference to securities registers. Financial instruments may be subscribed via the internet, but the customer's identity has to be confirmed before the securities are transferred to the customer's Central Securities Depository account.
- Where **"corporate finance" services** are concerned, an investment firm is considered to have established a customer relationship once it has entered into an agreement to accept an assignment (including counselling), arrangement, guarantee provision or other services. Customer identity therefore has to be verified before or upon the signing of a mandate agreement. The money laundering rules, including the identity verification requirement, apply to all assignments accepted by the investment firm in connection with its corporate finance business, for example assignments involving the preparation of offer documents and prospectuses, see the Securities Trading Act section 4-13 and section 5-5. Where assignments are executed without a written agreement, identity verification will take place when a verbal agreement is entered into, i.e. when the investment firm accepts the assignment.

Section 2, second paragraph, et seq. of the Money Laundering Regulations lists the points at which the customer relationship is considered to be established in the case of the new categories of reporting entities:

- **State authorised and registered auditors** are considered to have established a customer relationship once they have entered into an agreement to take on an assignment, including counselling and other services, or have sent an auditor's declaration to the Register of Business Enterprises. This means that the money laundering rules, including the requirement as to verification of customer identity, apply in principle to all assignments accepted by an auditor, for example to certification assignments accepted by the auditor under the Auditors Act section 1-1, third paragraph, second sentence.

- **Authorised external accountants** are considered to have established a customer relationship once they have entered into a written agreement on an assignment with a principal or an assignment requiring a written agreement, cf. the External Accountants Act section 3. According to this section assignment agreements with principals must be established in writing. Section 3 applies to external accountancy assignments. External accountancy is defined in the External Accountants Act as "*... the execution of a principal's duties pursuant to the accountancy legislation and the preparation of statements and information for the principal which the latter is required to furnish pursuant to law or regulations.*" Kredittilsynet is of view that the money laundering legislation will in principle apply to all assignments normally accepted by external accountants. It will also, for example, apply in cases where the external accountant does not perform the actual accounting function himself but confines himself to counselling. In such cases a condition is that the counselling is likely to be of significance for the preparation of statements and returns in the public sphere, for example income tax returns and accounts.

Kredittilsynet addresses the need for guidance on issues of special significance for auditors and external accountants in a separate circular. Such a circular will be published by the end of the first half of 2004.

- **Real estate agents, cooperative housing associations and lawyers engaged in real estate agency** are required by the Money Laundering Regulations to verify customer identity when a customer relationship is established in connection with a real estate agency assignment. According to the Estate Agency Act section 3-2, agreements on real estate agency assignments must be established in writing using the prescribed form. This means that a customer relationship is established when the assignment is signed, see the Money Laundering Regulations section 2, fourth paragraph. This applies to assignments both to sell and purchase a property. The identity of both the principal and the purchaser must be verified before the assignment is executed. The natural time for this to be done is when the contract is signed, and normally requires the purchaser to appear in person. If a contract meeting is not held, and the purchaser does not sign the contract in the real estate agent's presence, identity verification must be carried out via an outsourcing agreement in accordance with section 8, second paragraph, of the Money Laundering Regulations. It is sufficient for the real estate agent to obtain a copy of identity documents for property registration purposes and to retain the copy in the case file. The copy must be retained for ten years, cf the Estate Agency Regulations section 4-5 and the Money Laundering Regulations section 15, second paragraph.

### 2.3 Section 4 Requirements on identity documents etc (physical persons)

This section establishes the requirements on identity documents when a customer relationship is established with a physical person.

According to the Money Laundering Act section 5 first paragraph first sentence:

*“Persons or undertakings with a reporting obligation shall on establishment of a customer relationship request that the customer show valid proof of identity.”*

Moreover, section 4 first paragraph of the regulations requires the presentation of “*written proof of identity*” when a customer relationship is established. The Government introduced, on 9 March 2004, a Bill putting written (visual) proof of identity and electronic proof of identity on an equal footing (Act No. 81 on Electronic Signatures, which includes qualified certificates). Until the required amendments are made to the money laundering legislation, electronic proof of identity will not be regarded as valid proof of identity under this legislation.

Section 4 first paragraph requires identity documents to be produced in “*the original or as a certified copy*”. The general rule is that the identity documents are to be produced in the original. Only by way of exception will a “*certified copy*” be admissible, for example in cases where a person applying for a visa has to send the original identity documents to an embassy or consulate. Section 3 first paragraph of the previous Money Laundering Regulations (no. 118 of 7 February 1994) included a list of persons able to issue such confirmation: “*postal employees, including rural postmen, the police, lawyers, and state authorised and registered auditors*”. Other institutions as referred to in section 1 of the regulations, i.e. all institutions coming under the regulations, were also entitled to issue such confirmation. In practice the above-mentioned persons and institutions do not perform this function to any significant extent. Although the above-mentioned enumeration does not figure in the new Money Laundering Regulations, the persons and institutions in question will be entitled to issue such confirmation. All reporting entities under section 4 first and second paragraph of the Money Laundering Act, with the exception of the second paragraph no. 8 (dealers), will also be entitled to issue such confirmation. Kredittilsynet regards this enumeration as complete and exhaustive.

Section 4 first paragraph also sets out the data that identity documents have to contain. Not all such data need to be contained in one particular document. Presentation of several identity documents which in aggregate contain the proof of identity required will be considered sufficient.

In the case of physical persons the identity document(s) must contain:

- full name
- signature
- photograph
- personal identity number (11 digits), in the event a D-number, or in the case of diplomats and NATO personnel a separate personal identification number.

A D-number can be allocated to a physical person who does not meet the conditions for allocation of a personal identity number, and who has a customer relationship with a Norwegian bank or other institution subject to the rules of the Financial Institutions Act,

see the regulations on D-numbers adopted by the Directorate of Taxes on 14 February 1995. The institution in question is responsible for requisitioning the D-number.

According to the Money Laundering Act section 5 first paragraph, the identity document has to be "valid". Section 4 first paragraph states that identity documents must be issued by a public authority or by another agency whose control routines for the issue of documents are satisfactory, and whose documents are generally accepted as having a satisfactory level of security. Kredittilsynet interprets this provision to mean that identity documents must be recognised either as national, or correspondingly international (for example within the EEA). This means that cards issued locally, or for limited use within an undertaking, school or university, association etc cannot be accepted as valid proof of identity. Moreover identity documents must not have expired.

Identity documents deemed to meet the requirements as to verification routines and security level include:

- valid passport or other approved travel document
- bank card (Norwegian)
- driving licence – original and duplicate (not, however, a Norwegian “green driving licence”, which is now obsolete)
- Armed Forces ID card. This card will be superseded by a Ministry of Defence ID card in the course of 2004.
- Norway Post's ID card issued after 1 October 1994
- EU card
- Asylum seeker certificate. However, due to factors related to their issue and use, such certificates may, based on a concrete assessment, be deemed unsuitable for identity verification purposes.

A number of documents, such as bank cards issued in a particular period, do not contain a complete personal identity number (11 digits). If a document that lacks a complete personal identity number is presented, the institution will require proof of a personal identity number, for example a certificate of tax paid on declared earnings or a card issued by the National Population Register confirming the prospective customer's personal identity number.

Documents which **cannot** be regarded as meeting the requirements of the money laundering legislation include:

- credit cards, invoicing cards and the like
- Norway Post's identity cards issued prior to 1 October 1994
- travel pass for bus, tram, train etc.,
- association membership cards
- identity cards issued by schools or universities

In the case of physical persons who have not been allocated a Norwegian personal identity number or D-number, satisfactory proof of identity needs to be produced containing:

- the customer's full name
- date of birth
- place of birth
- sex
- nationality. If the reporting entity is aware that the customer has dual nationality, this must be registered as additional information.

Moreover, according to section 6 of the Money Laundering Act, the following data shall invariably be registered when a customer relationship is established:

- permanent address

According to section 4 last paragraph of the Money Laundering Regulations, the **obligation to produce proof of identity**, which is set out in the first paragraph, **also applies to** the person(s) authorised to operate the account or safe custody facility, or authorised to have the transaction carried out.

#### **2.4 Section 5 Cases where the customer is unable to produce identity documents**

This section, in exceptional cases, allows for the establishment of a customer relationship or for a transaction to be carried out even where the customer is unable to produce satisfactory proof of identity. The condition is that the institution is certain of the customer's identity, has reason to believe that the customer does not possess identity documents, and that requiring the customer to obtain such documents would be unreasonable in view of his/her age or state of health. Pertinent examples are accounts established for under-age persons, for example children to be christened. In such cases the reporting entity has to obtain and record the following data on the customer by other means in accordance with the Money Laundering Act section 6:

- 1 full name or name of company,*
- 2 personal identity number, organization number, D-number<sup>2</sup> or, if the customer has no such number, another unique identity code,*
- 3 permanent address,*
- 4 reference to proof of identity supporting the identity control<sup>2</sup>*

This section does not apply to “*persons who undertake large transactions on a regular basis*”. Although it might at the outset be difficult to know whether a customer relationship is in this category, reporting entities need to exercise due and proper judgement in the particular case. So-called collection accounts, for example for charitable organisations, should **not** be exempt from the requirements to produce identity

---

<sup>2</sup> The D-number corresponds to the five-digit Norwegian personal identity number, and is used by foreign nationals who do not hold a Norwegian personal identity number.

documents. Kredittilsynet also points out that when establishing a customer relationship with a legal person, reporting entities are required to comply with section 6 fourth paragraph of the Money Laundering Regulations requiring proof of identity to be produced “*by a physical person on behalf of the legal person*”. See the account of section 6 fourth paragraph for further details.

## 2.5 Section 6 Requirements on identity documents etc (legal persons)

This section establishes the requirements on identity documents that apply to legal persons.

- Legal persons registered in the Register of Business Enterprises need to produce a certificate of registration dating back no further than three months. Kredittilsynet considers the following documents acceptable to this end:
  - The original certificate, in the event a copy duly certified pursuant to the guidelines set out under section 4 above
  - A transcript of the original certificate telefaxed from the Brønnøysund Register Centre
  - A transcript of full and complete company data, dating back no further than three months, obtained from the Brønnøysund Register Centre by undertakings licensed by the Data Inspectorate to carry on credit information business (e.g. Dun & Bradstreet, CreditInform, Lindorff etc)
- In the case of a legal person registered in the Central Coordinating Register for Legal Entities but not in the Register of Business Enterprises, a transcript from the Central Coordinating Register for Legal Entities dating no further back than three months has to be presented that contains all registered data on the entity as mentioned in section 5 and section 6 second paragraph of the Act on the Central Coordinating Register for Legal Entities.
- A legal person not registered in the Central Coordinating Register for Legal Entities but in another public register needs to document evidence of similar, uniquely identifying characteristics, details of the legal person’s name (firm), the address of its place of business or head office and, if applicable, its foreign organisation number, and must also state which public register, within or outside Norway, can verify the information given.
- The last paragraph of this section establishes a new obligation to **verify identity** in accordance with section 5 of the Money Laundering Act, and to **register information** in accordance with section 6 of the same Act “*for a physical person on behalf of the legal person*”. This provision reads:

*“If it is clear or probable that the legal person is not registered in a public register, proof of identity shall be requested in accordance the Money Laundering Act section 5 and data shall be recorded for a natural person*

*on behalf of the legal person in accordance with the Money Laundering Act section 6.”*

This obligation is confined to the establishment of customer relationships with legal persons who are not registered in the Brønnøysund Register Centre. Typical examples here are associations, co-ownerships, investment clubs, charitable organisations, including collection accounts etc, to which the registration requirement set out in the Act on the Register of Business Enterprises does not apply.

Section 6 of the Money Laundering Regulations establishes a **registration requirement** for a physical person “*on behalf of the legal person*” in the reporting entity’s customer databases. This entails registering the customer relationship in the name of the physical person in question. Which physical person this happens to be will depend on the nature of the undertaking, including any delegation of authority to sign on its behalf and/or the designation of any disposition holder. The physical person may be the chief executive officer/general manager, board chairman or association chairman. Where the legal person does not have a chief executive officer/general manager, chairman or the like, the physical person may also be an associate, partner, co-owner, promoter, sub-manager or agent. This list is not exhaustive. If the registration requirement is not complied with, the customer relationship cannot be established. If the physical person in question is not a sub-manager and/or agent for the customer, he or she must also provide proof of identity, and register the information in accordance with sections 5 and 6 of the Money Laundering Act. The reporting entities must check that the customer has made a formal decision to entitle the physical person in question to sign on behalf of the legal person.

The intention behind the new provision requiring a physical person to verify his/her identity and to register on behalf of the legal person is to curb the allocation of made-up customer numbers when customer relationships are established. Financial institutions have in varying degrees allocated made-up customer numbers to legal persons who are not required to register. However, many institutions with a reporting obligation have urged such customers to register voluntarily in the Central Coordinating Register for Legal Entities and thereby be allocated an organisation number. Alternatively, reporting entities have encouraged a physical person who is associated with the legal person to "lend" his/her personal data for the purpose of registering the customer relationship.

A further justification for the new identity verification requirement is the FATF’s special recommendation no. 8 – “Non-profit organisations” – which addresses misuse of such organisations in connection with terrorist financing. Where measures to counteract misuse of such organisations are concerned, reference is also made to the FATF document of 11 October 2002, “Combating the Abuse of Non-Profit Organisations: International Best Practices”; see [www.fatf-gafi.org](http://www.fatf-gafi.org).

Although section 6 of the Money Laundering Regulations does not say so explicitly, in all cases where a legal person establishes a customer relationship with a reporting entity the identity of the person(s) who are to operate the account or safe custody facility has to be verified, cf the same requirement set out in respect of physical persons in section 4 last

paragraph of the Money Laundering Regulations. Reference is made to section 4 third paragraph of the Money Laundering Act which reads “*This Act also applies to persons and undertakings who perform services on behalf of or for persons or undertakings with a reporting obligation*”. Identity verification applies to all persons entitled to operate the account or safe custody facility, for example a procurist (Act no. 21 of 21 June 1985 on Procura), and the holder of “power of position” (*stillingsfullmakt*) or “dependent authority” (*oppdragsfullmakt*). The same applies to a person(s) entitled to execute an isolated transaction.

Where **limited companies in the process of incorporation** are concerned, and which have not been registered in the Register of Business Enterprises or the Central Coordinating Register for Legal Entities at the time of establishment or at the time of the transaction, Kredittilsynet expects the institution to request the company to present its incorporation document in the original. A copy of this document must be kept by the institution in accordance with section 15 of the Money Laundering Regulations. Moreover, the same form of identity document must be required as for physical persons mentioned in section 4 of the regulations, or for the person(s) authorised to operate the account or safe custody facility.

## **2.6 Section 7 Exceptions from the obligation to request proof of identity**

Section 7 first paragraph litra a) provides for exceptions from the identity verification requirement and the requirement to register data in cases where the customer is a financial institution, cf the Financial Institutions Act section 1-4 (commercial and savings banks, insurance companies, and mortgage credit institutions and finance companies), and in the case of investment firms and management companies for securities funds. Exceptions also apply to foreign institutions operating under corresponding rules that meet the identity verification requirements contained in Council Directive of 4 December 2001 on prevention of the use of the financial system for the purpose of money laundering (2001/97/EC), and which in addition are **subject to supervisory arrangements of EEA standard**. Countries with supervisory arrangements of EEA standard are assumed to include – alongside EU/EEA states – Australia, Canada, Hong Kong, Japan, New Zealand, Singapore, Switzerland, Turkey and the USA (all of which are members of FATF – the Financial Action Task Force on Money Laundering). The new countries joining the EU in the first half of 2004 will meet the requirements as to supervisory arrangements of EEA standard once they have the required rules in place. It has yet to be decided to what extent the supervisory arrangements of the new FATF countries – Brazil, Mexico, Argentina, and the latest member countries Russia and South Africa – are up to EEA standard.

### **2.6.1 Exceptions from the identity verification requirement in respect of certain insurance contracts**

According to section 7 b) to 7 e), insurance companies are not required to verify customer identity or to record data when establishing customer relationships in the cases listed in section 7 b) to e). The exceptions in question apply to cases where the risk of money laundering is considered to be slight, including in the case of insurance contracts involving small amounts.

Kredittilsynet's position here is that paid-up policies of less than 1G (the basic amount under the National Insurance Scheme) that are transferred to individual pension agreements (IPAs) also qualify for exception from the identity verification requirement set forth in section 7 d). Kredittilsynet also assumes that pension schemes under the Act on Defined Benefit Pension Plans (No. 16 of 24 March 2000) are excepted from the identity verification requirement.

However, the money laundering legislation's other provisions do apply to insurance companies, including the requirement to establish proper control and communication routines, personnel training and the investigation and reporting of suspicious transactions to ØKOKRIM. A money laundering officer ("senior manager responsible for money laundering affairs") must also be appointed.

## **2.7 Section 8 Verification of identity etc**

This section regulates verification of customer identity, including the checking of identity documents.

In the following an account is given of situations that call for verification of customer identity (2.7.1). This is followed by an account of the identity verification procedure (2.7.2).

### **2.7.1 Situations that call for identity verification**

**Section 5 of the Money Laundering Act** points to **three situations that call for reporting entities to verify customer identity**. The three situations are regulated in section 5 first, second and third paragraphs which read as follows:

1. *"Entities with a reporting obligation shall upon establishment of a customer relationship request that the customer show valid proof of identity."*

The stage at which a customer relationship is considered to be established is described under 2.2 (section 2) above.

2. *"As regards transactions involving NOK 100 000 or more concerning customers with whom the persons or undertakings obliged to report have no previously established customer relationship, proof of identity shall be requested as referred to in the first paragraph. The above threshold shall be assessed collectively in respect of transactions carried out in several operations that appear to be associated with each other. If the transaction amount is not known when the transaction is carried out, identity verification shall be performed as soon as the entity with a reporting obligation becomes aware of the amount and that it exceeds the threshold."*

The term "transaction" is defined in the Money Laundering Act section 2 subsection 2 as including "any transfer, intermediation, exchange or placement of assets".

3. *“The entity with a reporting obligation shall in all cases request proof of identity as referred to in the first paragraph if he or she suspects that the transaction is associated with the proceeds of crime or with offences covered by section 147a or section 147b of the Penal Code.”*

The obligation to verify customer identity comes into play the **very first time that a customer relationship is established**, cf alternative no. 1 in the Act. Customer relationships do not comprise isolated transactions, cf alternative no. 2 in the Act. Such transactions may, according to the circumstances, come under the identity verification requirement under alternative 2 and 3 above. Customer identity does not have to be verified upon any subsequent enlargement of customer relationships in the same institution (e.g. opening a new account, writing a new insurance policy etc). However, the institution must be certain of the identity of customer in connection with any customer care implementation or any enlargement of the customer relationship.

The obligation to verify customer identity applies to the establishment of **all** customer relationships, including where services are provided via telephone, the internet etc.

The obligation to verify the identity of new customers applies regardless of the amount involved.

Entities with a reporting obligation that form part of a group have independent obligations and cannot automatically rely on identity verification performed by another institution within the group. An entity with a reporting obligation may however enter into an agreement with other reporting entities within the group whereby the latter perform identity verification as authorised in section 8 second paragraph of the regulations, see below.

A group of companies may perform joint identity verification provided the customer relationships in question are established simultaneously. A condition for approving such verification is that each legal entity within the group retains a copy of the identity documents in accordance with section 15 of the regulations, see below. Identity verification carried out *previously* by another reporting entity (within or outside the same group) may, however, not be taken as a basis when establishing customer relationships.

The obligation to verify customer identity that is triggered by transactions involving NOK 100 000 or more pursuant to the Money Laundering Act section 5 second paragraph does not apply to an account holder's deposits or withdrawals from his/her own account.

The obligation to verify customer identity that is triggered by transactions involving more than NOK 100 000 in the case of customers who have not already established a customer relationship applies regardless of whether the transaction is performed as a single operation or as a number of operations that are assumed to be inter-related. In this context an institution comprising more than one branch is regarded as a single institution. Thus a branch that accepts an assignment is obliged to view this assignment in the context of any other executed transactions of which it is aware.

### 2.7.2 Implementation of identity verification

Section 8 first paragraph of the Money Laundering Regulations regulates the actual implementation of identity verification, in which the "know your client" principle stands at centre-stage. When a customer relationship is established with a reporting entity, the customer may gain access to the financial system. That is why identity verification is a crucial aspect of measures to combat the laundering of criminal proceeds and terrorist financing. Proper verification of customer identity will necessarily entail use of resources and costs for the individual institution. In addition to counteracting money laundering and terrorist financing, a smoothly functioning identity verification regime can also help to reduce institutions' counterparty risk and thereby the risk of financial loss and loss of reputation.

As a general rule of identity verification, the customer is required to appear **in person at the premises of the primary undertaking**, i.e. of the undertaking that enters into the agreement in the customer, to enable the institution to check that the customer's appearance and name match the photograph and name appearing in the identity documents. See section 5 fourth paragraph first sentence of the Money Laundering Act. If the primary undertaking does not have a branch network, for example where financial services are offered electronically, the primary undertaking is entitled under section 8 second paragraph of the Money Laundering Regulations to outsource identity verification to undertakings and legal persons listed in the Money Laundering Act section 4 first and second paragraph. In this case too, identity verification must be based on the customer's appearance in person at the premises of the undertaking to which identity verification is outsourced.

According to the Money Laundering Act section 5 fourth paragraph second sentence there are **two types of cases** in which reporting entities can **make exceptions from the requirement as to personal appearance** at the premises of the primary undertaking for the purpose of identity verification. The provision reads as follows:

*“If personal appearance constitutes a major inconvenience for the customer or is not practicable, an exception may be made from this requirement provided that satisfactory identity control can nevertheless take place.”*

1 The first exception relates to the **customer's circumstances**. This exception applies to situations in which it would be highly problematic or burdensome for the customer to appear for identity verification in person, for example due to illness or old age. This exception is elaborated on under 2.7.2.1 below.

2 The second exception, relating to the **undertaking's circumstances**, applies in cases where appearing at the primary reporting entity in person is practicable. This exception is detailed below under 2.7.2.2. In order for the requirement as to satisfactory identity verification under the Money Laundering Act section 5 fourth paragraph second sentence (see above) to be met, the

reporting entity will in this case need to follow the procedure described in the Money Laundering Act section 8 second paragraph, which permits the primary undertaking to enter into a written agreement (general or in isolated cases) with the undertakings and legal persons listed in the Money Laundering Act section 4 first and second paragraph. Such an agreement entails outsourcing identity verification, and is described in further detail below. The primary undertaking is still responsible for ensuring that identity verification is carried out in accordance with law and regulations. This method of identity verification can for example be used by reporting entities that do not have a branch network, including where reporting entities offer their services electronically.

#### **2.7.2.1. Exceptions where appearing in person would cause the customer major inconvenience**

The first alternative under the Money Laundering Act section five fourth paragraph second sentence enables personal appearance at the institution to be dispensed with if such appearance would cause the customer "major inconvenience", and satisfactory verification can nevertheless be carried out. The use of the term *major* means that it must be extremely burdensome for the customer to appear at the institution in person.

The fact that identity verification has to be satisfactory is an absolute requirement which also applies in cases where personal appearance would constitute a major inconvenience to the customer.

Possible exceptions include:

- Where a person is unable to travel due to illness, handicap or similar situation which precludes personal appearance at the institution
- Where a person has been placed in a prison institution
- Where geographical distance may bring the excepting provision into play

Personal appearance is fundamental to the identification process. Where a major inconvenience exists, the institution should examine the feasibility of visiting the customer, i.e. of verifying the customer's identity at a meeting with the customer. In this case too the requirement is that satisfactory verification can be carried out.

#### **2.7.2.2. Exceptions where personal appearance at the primary undertaking is not practicable**

In this case exceptions may be made from the requirement as to personal appearance at the primary undertaking, i.e. the undertaking stated in the financial agreement or a corresponding agreement with other reporting entities. A condition for dispensing with the requirement as to personal appearance at the primary undertaking is that **satisfactory identity verification is carried out by personal appearance at another reporting entity** in connection with outsourcing pursuant to the Money Laundering Regulations section 8 second paragraph:

*“An entity with a reporting obligation may, pursuant to the Money Laundering Act section 4 first and second paragraph, enter into a written agreement with another entity with a reporting obligation regarding verification of identity that entities with a reporting obligation are obliged to perform under the first paragraph above. In such cases the primary entity with a reporting obligation is responsible for ensuring that identity verification is carried out in due and proper manner in accordance with law and regulations and for establishing proper routines in accordance with section 10 fourth paragraph and section 16.”*

This method of identity verification entails that the primary undertaking outsources identity verification to the undertakings/individuals listed in the Money Laundering Act section 4 first and second paragraph. The listing is reproduced above under section 1. The money laundering legislation also provides for identity verification to be left to undertakings/individuals other than those stated in section 4 first and second paragraph. In such cases agents and independent distributors of reporting entities' products may carry out identity verification on behalf of a reporting entity (not outsourcing). The activity of such agents is regulated in Kredittilsynet's circular 37/94 of 30 August 1994 entitled "Concerning the use of agents, disclosure obligation to borrowers and accounting for setting-up charges". Point 1.1 of the above circular requires financial institutions to notify such agency relationships to Kredittilsynet. According to the Money Laundering Act section 4 third paragraph, *"This Act also applies to persons and undertakings who perform services on behalf of or for persons or undertakings with a reporting obligation."* In such cases reporting entities have **full and complete responsibility** for ensuring that agents and independent distributors act in accordance with the money laundering legislation, which includes ensuring that identity verification and training of all persons who perform such services are implemented in a proper manner.

### **2.7.2.3. Further details on the outsourcing of identity verification**

Section 8 second paragraph of the Money Laundering Regulations requires **such agreements to be in writing**. Such an agreement should be formulated in accordance with the principles listed in the bullet points below. Furthermore, the agreement should require persons implementing identity verification on behalf of the primary undertaking to make a copy of the identity documents, stamp each of them with “certified true copy”, endorse them with the name in block capitals of the staff member who has performed the identity verification, as well as sign for having performed the identity verification, and to send this material to the primary undertaking that established the customer relationship. Kredittilsynet has noted that the quality of copies of identity documents varies. Kredittilsynet would emphasise that the photograph, stamp, name and signature shown in copies must be easily legible. The primary undertaking is required to retain such data by section 15 of the Money Laundering Regulations.

General non-statutory principles and conditions for outsourcing set out in NOU 2001:23 "Financial institutions' activity", chapter 5, p. 28-30: "Outsourcing of services", will apply in such cases. The following points should be noted:

- The reporting entity's management board retains responsibility for the activity that is outsourced.
- The reporting entity's management board must have established guidelines for the outsourcing.
- The agreement with the commissioned party must provide the necessary basis for information to, and for inspection and supervision by, the supervisory authorities in the same way as when the reporting entity itself performs the activities in question.
- The activity to be outsourced must be stated in a written agreement. The agreement must entitle the reporting entity to instruct the commissioned party and to audit the outsourced activity.
- The reporting entity itself must have the competence to assess whether the commissioned party is performing the assignment satisfactorily.
- The reporting entity shall throughout have the opportunity to identify and control risks associated with the outsourcing of assignments.
- The reporting entity shall have a plan for resolving problems which may arise should the commissioned party be unable to carry out the assignment.
- The reporting entity must secure a reasonable right to terminate the agreement under satisfactory conditions until an alternative solution has been established.

#### **2.7.2.4 Outsourcing in the securities field**

The following regulations regulate outsourcing in securities field:

Regulations no. 289 of 7 March 2003 on investment firms' use of commissioned parties (outsourcing).

Regulations no. 798 of 8 July 2002 on the use of commissioned parties by management companies for securities funds (outsourcing).

#### **2.7.2.5 Outsourcing of identity verification to Norway Post's branch network**

Where identity verification is outsourced to Norway Post (or other postal operators), see the Money Laundering Act section 4 first paragraph no. 9, the **following method will meet the requirements as to identity verification:**

Norway Post's branch network performs identity verification on behalf of entities with a reporting obligation (outsourcing). Norway Post terms this method "Personal Collection with Receipt" (Norwegian acronym: PUM). In order for this arrangement to comply with section 15 fourth paragraph of the new Money Laundering Regulations (see comment below), which requires "*copies of presented identity documents*", the reporting entity

must take care to revise its arrangements such that Norway Post's branches take a photocopy of the identity documents when identity verification is carried out. The right, as provided for in the earlier Money Laundering Regulations, to make a written copy of the relevant data contained in the identity documents does not apply in the new regulations.

Identity verification is performed by a letter being sent from the reporting entity to the customer by registered first-class mail. When the letter is collected, the recipient (customer) confirms receipt of the letter with his/her signature. A photocopy must be taken of the recipient's proof of identity. Norway Post's customer service personnel confirm the handover of the letter with their signature and a "certified copy" stamp. A copy of the identity document is thereafter returned to the reporting entity in a closed envelope. These documents, which are proof that identity verification has been performed, must be retained under section 15 of the Money Laundering Regulations by the primary reporting entity which has entered into the agreement with the customer. It should be stressed that the primary undertaking has the full and complete responsibility for ensuring that identity verification is carried out in a proper manner in compliance with the money laundering legislation.

Until such time as Norway Post has brought its method of identity verification into line with the Money Laundering Regulations, Kredittilsynet may, in a transitional period, approve a written copy to be made of relevant data contained in identity documents. A condition is that the customer sends a copy of the identity document in question to the primary undertaking, and that the undertaking checks that the photocopy matches Norway Post's written copy of the reference number etc. The primary undertaking is also required to retain this photocopy under section 15 of the Money Laundering Regulations.

Norway Post has outsourced the provision and performance of various financial (and postal) services, including identity verification, to shops in the retail market ("Post Office in Shop"). Kredittilsynet has no objections to such outsourcing, provided that this activity is operated in accordance with the money laundering legislation and the guidelines set out in this circular. Only shop staff with proper training corresponding to that required by section 16 of the Money Laundering Regulations may provide such services.

Section 6 last paragraph of the Money Laundering Act imposes on reporting entities an independent duty to ascertain and record the data required by the first and third paragraph of this section. The condition underlying this obligation is that the reporting entity knows or has reason to believe that the customer is acting on behalf of another entity, or that another entity owns the capital item that is the subject of the transaction.

Where a person resident, or undertaking established, abroad intends to establish a customer relationship with a Norwegian undertaking with a reporting obligation, the Norwegian reporting entity may enter into isolated agreements or a general agreement with a foreign reporting entity on such identity verification. A condition here is that the foreign undertaking meets requirements corresponding to FATF's revised

recommendations, and is in addition subject to a supervisory arrangement of EEA standard.

Where banks' use of self-service deposit terminals is concerned, Kredittilsynet expects software to be installed requiring the customer or other user to use a pin code when performing transactions on such terminals. A condition for using such terminals is that identity verification has been carried out in accordance with section 8 of the Money Laundering Regulations when the customer relationship is established.

Requirements as to identity verification are not exhaustively regulated in the money laundering legislation. Section 3 of Regulations no. 1751 of 19 December 2003 on notification and reporting of payments between residents and non-residents etc., to Norges Bank reads as follows:

*"In connection with payments between residents and non-residents through a foreign exchange bank or a foreign exchange undertaking, such bank or undertaking is required to assure itself of the customer's identity and of whether the customer is a resident or non-resident.*

*In connection with the purchase or sale of foreign currency, the foreign exchange bank or foreign exchange undertaking in question is required to assure itself of the customer's identity and of whether the customer is a resident or non-resident."*

#### 2.7.2.6 Practical examples of implementation of identity verification

- **Subscribing mutual fund units just before year-end** may mean that it is not "*practicable*" to appear in the institution in person when the order is submitted. This is because many thousands of such contracts are entered into close to the end of the year, and it is not desirable to impose on the institution the extra burden of having to dramatically increase staff resources in this period. The institution will have to verify the identity of new customers in the regulation manner as soon as this can be done.
- A number of undertakings with a reporting obligation frequently establish **customer relationships outside their own branches**, for example finance companies where the customer relationship is established via the purchase of a product from a dealer and the dealer verifies the customer's identity on behalf of the financial institution. **The new money laundering legislation continues this practice.** According to section 8 second paragraph of the Money Laundering Regulations reporting entities, including finance companies, can enter into an agreement in writing with another reporting entity, including dealers, cf section 4 second paragraph no. 8, on implementation of identity verification on behalf of the primary undertaking.

Although section 4 second paragraph no.8 of the Money Laundering Act ("dealers") refers to "*cash transactions of NOK 40 000 or more or a corresponding amount in foreign currency*", the rules must be understood such that it is also possible for a finance company to enter into such agreements in writing on identity verification with dealers in respect of amounts below NOK 40 000, and in cases where the customer wishes, say, to be issued with a payment card.

If the finance company has not verified the customer's identity, the dealer does so in the finance company's place and forwards the documents to the financial institution. In this context the dealer acts as an agent for the institution. Kredittilsynet wishes to make clear that it is the institution which establishes the customer relationship that is responsible for compliance with the provisions in question, and for the carrying out satisfactory verification of identity. Where agents are used in this manner in the identity verification process, the institution must see to it that the Money Laundering Regulations' requirement as to training, cf section 16, and as to the establishment of proper internal control and communication routines, cf section 13 of the Money Laundering Act, are met in these cases. Kredittilsynet may ask the institution in question to produce documentary evidence that this has been done.

Kredittilsynet advises that agreements on identity verification may also be entered into with dealers in cases not involving sales financing.

- Where **issuance of securities** is concerned, the lead manager or other office of issue is required to carry out identity verification. This does not apply where the customer intending to participate in the issue subscribes through his regular business connection (an institution subject to these regulations) and identity verification is carried out there. If the customer contacts the office of issue directly, identity verification must be carried out at the office of issue in question, unless this has been done previously. However, the office of issue may apply section 8 second paragraph of the Money Laundering Regulations if it does so simultaneously with subscription.

Identity verification must be carried out before any securities allocation is transferred to the customer's Central Securities Depository account. Subscription where settlement is affected via an already established bank account is regarded as an isolated transaction and the obligation to prove identity does not rise. This obligation will, however, arise where subscription totals NOK 100 000 or more, or where there is reason to believe that the subscription is related to criminal proceeds, cf the Money Laundering Act section 5, second and third paragraph.

## **2.8 Recapitulation – identity verification**

The money laundering legislation does not authorise other methods of identity verification than those described in this circular. Entities with a reporting obligation that practise identity verification methods that diverge from those described in this circular

must immediately initiate changes to bring their identity verification procedures into line with the Money Laundering Act and associated regulations.

## **2.9 Section 9 Absence of, or inadequate, proof of identity - refusing the customer**

An entity with a reporting obligation must refuse to establish a customer relationship or to carry out a transaction if identity documents produced by the customer fail to meet the requirements of section 4 of the Money Laundering Regulations, or there is reason to believe that the identity documents are not correct and verification as mentioned in section 8 does not disprove such suspicion or cannot be carried out.

Establishing a temporary customer relationship on the understanding that the customer will produce satisfactory proof of identity at a later stage is not permitted.

Should suspicion arise, in a situation as described in this section, that the transaction is related to a criminal offence or to circumstances coming under the Penal Code sections 147a and 147b, the institution is required to undertake investigations to confirm or disprove its suspicion under section 10 of Money Laundering Regulations. If the investigations do not disprove the suspicion, the institution shall on its own initiative forward all information on circumstances that may indicate such a violation to ØKOKRIM in accordance with section 11 of Money Laundering Regulations. The same applies if the customer's identity is in doubt.

## **2.10 Section 10 Investigation of suspicious transactions**

This section refers to the Money Laundering Act section 7 first paragraph which requires reporting entities and their employees to make investigations if a transaction is suspected of being related to criminal proceeds or to circumstances coming under the Penal Code sections 147a and 147b.

It follows from section 7 second paragraph that if suspicion is not disproved, the reporting entity shall report the transaction to ØKOKRIM.

Section 7 “Obligation to investigate and report” reads as follows:

*“If an entity with a reporting obligation suspects that a transaction is associated with the proceeds of crime or with offences covered by section 147a or section 147b of the Penal Code, further investigations shall be made in order to confirm or disprove the suspicion. This obligation also applies to employees of entities with a reporting obligation.*

*If the investigations fail to disprove the suspicion, the entity with a reporting obligation shall on its own initiative submit data concerning the transaction in question and the matters that have given rise to suspicion to the National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway (ØKOKRIM). The entity with a reporting obligation and its*

*employees shall, if so required, provide ØKOKRIM with all essential data concerning the transaction and the suspicion.*

*Customers or third parties shall not be informed that data has been provided to ØKOKRIM.”*

The Money Laundering Regulations do not contain a definition of a "suspicious transaction". Section 10 first paragraph of Money Laundering Regulations specifies various circumstances which may trigger the obligation to investigate. The following overview is not exhaustive.

- **The transaction appears to lack a legitimate purpose.** It may for example involve an assignment in which the sum of money is to move back and forth between different accounts within a given period, that the same amount is to move back and forth between different institutions in accordance with a given assignment, and that a sizeable sum is split into a number of smaller sums, but is reunited in a new account.
- **The transaction is unusually large or complex, or is unusual in relation to the customer's habitual business or personal transactions.** Here a concrete assessment needs to be made. A transaction may be large in relation to one customer, but quite normal in relation to another. Institutions will have to apply their knowledge of the individual customer. The "know your client" principle is crucial here.
- **The transaction involves a transfer to or from a customer in a country or area lacking satisfactory measures against money laundering or terrorist financing.** Here particular diligence must be shown in relation to transactions outside the FATF area. There is particular reason to be alert to transactions with customers or institutions in countries with strict secrecy laws that offer high returns and tax exemption. Under the heading "NCCT initiative", FATF's website, at [www.fatf-gafi.org](http://www.fatf-gafi.org), carries an overview of useful background information on measures against countries and areas which are not collaborating in the fight against money laundering and terrorist financing ("Non cooperative Countries and Territories"). FATF also publishes a list of such countries and territories. Changes in this list are published on Kredittilsynet's website. Money laundering officers at reporting entities should access Kredittilsynet's website to stay updated in this field. Reference is also made to Kredittilsynet's circular 22/2003 "Handling of lists from the UN and FATF and similar announcements – changes in Kredittilsynet's practice", dated 29 August 2003.
- **The transaction is otherwise of an anomalous nature.** This requires a concrete assessment in the individual case. The following examples are mentioned:
  - Rapid and extraordinary repayment of loans in cash

- A significant disparity between documented debt-servicing ability in terms of income, financial assets etc., and the amount owed and agreed repayment conditions (extraordinary repayment), may indicate money laundering.
- Use of bank drafts that are repeatedly renewed
- Large-scale exchange of old banknotes that have become invalid
- Use of unusual means of payment in relation to the underlying operation
- Large cash transactions
- Use of payment cards to carry out an unusually large number of transactions over a short period.

Foreign exchange operations are an area that is particularly vulnerable to abuse for money laundering or terrorist financing purposes. Such operations include foreign currency exchange and payment transfers to foreign countries. Reference is made to a detailed discussion on pp 54-64 in Proposition to the Odelsting no. 81 (2002-2003).

The above indications of possible money laundering are to be viewed as examples. Actual techniques used are probably wider in number. This area is developing apace, and institutions need to be alert to and take account of new trends and methods in their training programmes. FATF's internet website contains useful information on such cases under the heading "Other Documents – Money Laundering Trends and Techniques".

There is reason to keep a special eye on business areas where there is little or no face-to-face contact with the customer. Institutions must also be able to fulfil their investigative obligations where the internet or other electronic systems are used by customers.

The obligation set out in the Money Laundering Act section 7 first paragraph for reporting entities to investigate suspicious transactions comes into play when the transaction is suspected of being related to criminal proceeds or to circumstances coming under the Penal Code sections 147a and 147b. According to the Money Laundering Regulations section 10 second paragraph, neither the customer nor any third party should be informed that such investigations are in progress. Section 7 third paragraph of the Money Laundering Act states that neither customers nor third parties should be informed that information has been passed on to ØKOKRIM. In some cases it may be natural to ask the customer questions able to confirm or disprove a suspicion. Since the point of departure is that the customer should not be made aware that investigations are in progress, the institution should proceed with caution in such situations.

Where an institution undertakes out-of-house investigations, it must take care to maintain statutory secrecy in regard to customers' private and business circumstances etc. This applies both in relation to other institutions and to public authorities in Norway and elsewhere. The Money Laundering Act section 11 second paragraph includes a new provision whereby entities with a reporting obligation under section 4 first paragraph no.1 of the act (financial institutions) are, notwithstanding the secrecy requirement, entitled to "*exchange necessary customer data when this is regarded as a necessary step in investigations of suspicions that a transaction is associated with the proceeds of crime or with offences covered by section 147a or section 147b of the Penal Code.*"

Kredittilsynet's position is that a similar opportunity to exchange information applies to insurance companies. Institutions are duty-bound to record the results of investigations, and the results must be available to Kredittilsynet at all times.

Section 10 fourth paragraph requires institutions to establish satisfactory internal control and communication routines ensuring compliance with the obligation to investigate. They are also required to draw up internal reporting systems whereby employees and others who perform such functions and who become aware of suspicious circumstances as mentioned in the first paragraph are required to report to their superiors and to a money laundering officer, i.e. a senior manager who is assigned responsibility for money laundering matters (see below under 2.11). Institutions need to take steps to ensure that their employees receive satisfactory training, and see to it that the institution at all times has a sufficient focus on anti-money laundering measures (cf the requirements of section 16).

Section 10 last paragraph is a new provision requiring reporting entities to retain data for at least five years on cases of possible suspicious transactions which employees and others have reported to the money laundering officer but which were not referred to ØKOKRIM.

#### **2.11 Section 11 Submission of data to ØKOKRIM**

Where suspicion as referred to in the Money Laundering Act section 7 first paragraph (see above under section 10) is not disproved by investigations, the transaction in question must be reported to ØKOKRIM in accordance with section 7 second paragraph of the same act. Only data on transactions that are suspected of being related to criminal proceeds or to circumstances coming under the Penal Code sections 147a or 147b need to be submitted to ØKOKRIM.

Section 11 first paragraph states that the reporting entity's money laundering officer is responsible for reporting to ØKOKRIM; see the Money Laundering Act section 13 third sentence. Kredittilsynet points out that each undertaking with a reporting obligation shall have a designated money laundering officer at senior manager level. In financial groups, all legal entities subject to the money laundering legislation are required to have a money laundering officer. The financial group may also have a money laundering officer at the group level. A necessary requirement is that the money laundering officer is located at a level at which he/she has sufficient powers to discharge his/her statutory tasks, and that gives him/her the thrust and effectiveness needed vis-à-vis the institution's employees and top management. At the same time the money laundering officer needs to devote enough of his/her working time to maintaining contact with the segment of the reporting entity's employees etc., who perform customer-service functions.

Section 11 first paragraph of the Money Laundering Regulations requires data on suspicious transactions to be transmitted to ØKOKRIM using a standardised form prescribed and approved by ØKOKRIM. Such a form is enclosed with this circular together with instructions. The form should be submitted by post or telefax (for institutions in the Oslo area the form can be delivered in person to ØKOKRIM). Ordinary e-mail

cannot be used because of the risk of information tapping. The form is also available at ØKOKRIM's website, [www.okokrim.no](http://www.okokrim.no).

ØKOKRIM's money laundering unit is manned throughout working hours, and can be contacted directly by phone for guidance on the money laundering legislation or if the caller is aware of suspicious transactions which may need to be reported.

The fact that an entity with a reporting obligation reports such information to ØKOKRIM in good faith in accordance with the Money Laundering Act section 7 second paragraph does not constitute a breach of the institution's duty of secrecy, and cannot provide a basis for bringing the institution or its employees to account, cf. section 11 first paragraph of the Money Laundering Act.

Where investigations are initiated under the Criminal Procedure Act, the documentation received by ØKOKRIM as enclosures to reports from institutions is frequently included in case documents. Hence where such documentation is concerned, vouchers should not be endorsed with crossings-out, nor should personal comments be written on statements of account etc.

## **2.12 Section 12 Electronic monitoring systems**

Section 12 requires financial institutions to establish electronic monitoring systems by the end of 2004. This provision is new to the money laundering legislation.

The obligation to establish such systems applies to the following financial institutions:

- 1 Savings banks and commercial banks.
- 2 Mortgage credit institutions and finance companies licensed under chapter 3 of the Financial Institutions Act.
- 3 Branches of credit institutions (banks, mortgage credit institutions and finance companies) within the EU/EEA. Based on the principle of mutual recognition set out in the Consolidated Banking Directive (2000/12/EC), such credit institutions can establish branches in Norway provided they are authorised, and subject to supervision, by the authorities in their own state.
- 4 This item covers Norwegian-registered branches or undertakings of foreign credit institutions (banks, mortgage credit institutions and finance companies) whose head office is in a state outside the European Economic Area, and which are authorised by Norwegian authorities to engage in financing activity in Norway. Hence this item covers financial service providers headquartered in countries outside the EU/EEA which have established such business in Norway.

Section 12 makes it clear that the purpose of such monitoring systems is that of *"identifying transactions suspected of being related to the proceeds of crime or to*

*circumstances coming under the Penal Code section 147a or section 147b.*" Examples of such possible transactions are listed under section 10 above.

The transactions identified by such systems must be checked and followed up manually before, in the event, being reported to ØKOKRIM. **An electronic monitoring system is an aid to discovering possible suspicious transactions.** Regardless of the existence of such systems, reporting entities, their employees, and other persons employed by the undertaking in such functions, have an **independent duty** to investigate suspicious transactions, and otherwise to act in accordance with the money laundering legislation.

According to Regulations no. 1057 of 20 June 1997 relating to the verification of control responsibilities, documentation and confirmation of the internal control system, financial institutions are responsible for establishing satisfactory in-house internal controls, also in the money laundering sphere. The institution's internal controls are a continual process – initiated, implemented and monitored by the undertaking's directors, management and other employees. General requirements on undertakings' internal control systems, which also include routines in the money laundering field, are set out in the annex to Kredittilsynet's circular 16/2003 "Guide to the internal control regulations".

### **2.13 Section 13 Special reporting of transactions associated with countries or areas which have not implemented satisfactory anti-money laundering measures etc.**

This provision is new to the money laundering legislation. It empowers the Ministry of Finance, subsequent to a decision from the FATF, to impose *“a special, systematic obligation to report to ØKOKRIM transactions with or on behalf of persons or undertakings associated with countries or areas which have not implemented satisfactory measures against the laundering of proceeds of crime or circumstances coming under the Penal Code section 147a or section 147b.*

Section 10 first paragraph of the Money Laundering Regulations requires entities with a reporting obligation to report to ØKOKRIM in accordance with section 11 of the Money Laundering Regulations should suspicion not be disproved by investigations. Among the circumstances which can prompt investigation are transactions which *“involve a transfer to or from a customer in a country or area lacking satisfactory measures against money laundering or terrorist financing”*. Section 13 of the Money Laundering Regulations provides for *“a special, systematic obligation to report”* such transactions regardless of whether the transaction appear suspicious in the meaning of section 10 first paragraph of the Money Laundering Regulations. A reporting obligation will be adopted by the Ministry of Finance in the form of regulations and will be announced in the Norwegian Law Gazette. The regulations will also be published on Kredittilsynet's website, [www.kredittilsynet.no](http://www.kredittilsynet.no).

### **2.14 Section 14 Prohibition of or restrictions on the right of reporting entities to establish customer relationships with or undertake transactions to or from countries which have not implemented satisfactory anti-money laundering measures etc.**

Section 14 of the Money Laundering Regulations, which is also new to the money laundering legislation, empowers the Ministry of Finance, in response to a decision by FATF, to impose a special prohibition or restrictions on the right of entities with a reporting obligation to establish customer relationships with or carry out transactions with persons or undertakings associated with countries or areas described under section 13 above.

### **2.15 Section 15 Requirement as to retention and deletion of data etc.**

This section requires entities with a reporting obligation to retain data as mentioned in sections 4, 6 and 8 of the Money Laundering Regulations for five years after termination of the customer relationship or after the transaction is carried out. According to the second paragraph of this section there is nothing to prevent other provisions of law or regulations from establishing longer periods for data retention, for example in the case of estate agency assignments where documents have to be retained for ten years.

The third paragraph of this section states that documents and data retained by entities with a reporting obligation must be deleted within one year of the retention obligation's expiry.

The Money Laundering Regulations state that information contained in identity documents as mentioned in section 4 of regulations ("physical persons"), and section 6 ("legal persons") shall only be retained "*in the form of copies*" of the presented identity documents. Hence the opportunity provided in section 7, alternative II, of the previous Money Laundering Regulations make a written copy of relevant data contained in the presented identity documents, and a reference to the documents, no longer applies.

Moreover, the copy of the identity document shall show the following details:

- Who (undertaking and person) has carried out the verification of identity – name in block capitals, the signature of person concerned and a "true copy certified" stamp
- The date of identity verification

The fifth paragraph of this provision states that "*entities with a reporting obligation shall retain data by such means as ensure that the documents do not lose their value as evidence*".

Where the **physical retention** of such documents is concerned, entities with a reporting obligation are required to ensure proper storage against fire, theft, frost, flooding and other external influences. Moreover, storage must be systematic to ensure that the appropriate document can actually be retrieved.

Where **non-paper based, for example electronic, retention** of such data and documents is concerned, the fifth paragraph of this section requires to entities to ensure that storage complies with regulations no. 1156 of 16 December 1992 (the "Loose-leaf Regulations")

sections 5-3 and 5-4. Section 5-3 first paragraph makes reference to which mediums must be used for storing documents and data:

**"Section 5-3** *Accounting material shall be stored using mediums as mentioned in section 1-1 point 1, 2 or 3. When called for on special grounds, storage using mediums as mentioned in section 1-1 point 4 may also be acceptable. Kredittilsynet may give approval for this to be done in the individual case and may impose further requirements on such storage.*

*The accounting material shall:*

*- be stored in an easily accessible location to permit checking during the period of storage. It shall be organised in a manner that permits efficient follow-up of the accounts and the documentation. It shall be properly secured to prevent damage and alteration.*

*- be easily legible directly with the aid of a computer screen/reading machine throughout the period of storage."*

Although it is not made clear in the text of the Money Laundering Regulations, Kredittilsynet's competence under section 5-3 first paragraph to give such authorisation is transferred to the Directorate of Taxes.

Section 1-1 no. 1, 2, 3 and 4 of the Loose-Leaf Regulations reads as follows:

**"Section 1-1** *Entities required to maintain accounting records who use loose-leaf books and other aids instead of bound books shall follow the rules of chapters 3, 4 and 5 of the regulations.*

*In this context, loose-leaf books and other aids include:*

- 1. Loose cards, sheets, journals and lists made of paper and other filing material which can be read directly.*
- 2. Microfilm and other filing material which can be read with the aid of magnification.*
- 3. Optical mediums (WORM) or equivalent non-erasable mediums.*
- 4. Erasable mediums."*

Section 5-4 of the Loose-Leaf Regulations establishes reporting entities' obligations in relation to the supervisory authorities:

**"Section 5-4** *Entities required to maintain accounting records shall at the request of the supervisory authorities provide assistance free of charge, including making available the equipment and software needed to verify the accounts.*

*The accounting material shall at the request of the supervisory authorities be presentable on paper for up to 3½ years after the end of the accounting year."*

Section 15 last paragraph of the Money Laundering Regulations requires reporting entities to "ensure that documents are secured so as to protect them against unauthorised access." In this connection reference is made to Act no. 31 of 14 April 2000 relating to the Processing of Personal Data (Personal Data Act) with appurtenant regulations which regulates these matters. Section 1 (purpose clause) of this act reads:

*"The purpose of this Act is to protect natural persons from violation of their right to privacy through the processing of personal data.*

*The Act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality."*

The Data Inspectorate has the administrative responsibility for the above legislation.

#### **2.16 Section 16 Training of employees etc., of reporting entities**

This section requires undertakings with a reporting obligation to ensure adequate instruction, training, maintenance and upgrading of employees' knowledge of the money laundering legislation, and of measures against terrorist financing. **This obligation applies to all persons who perform services on behalf of or for reporting entities, including substitutes and other temporary labour.**

The training of employees of entities with a reporting obligation is a key element of the measures to combat money laundering and terrorist financing and forms part of the requirements as to internal control and communication routines that are established in section 13 of the Money Laundering Act and section 16 of the Money Laundering Regulations. Hence it is important for reporting entities to maintain sufficient focus on this aspect.

Training is a process that needs to be implemented regularly to familiarise new staff with the legislation and their obligations. Staff who have already undergone training may also need to be updated on the rules applying at any time in this field. Entities with a reporting obligation should evaluate staff training needs on a continual basis. Reporting entities must also maintain a conscious awareness of what training is most appropriate to their particular institution, for example in terms of their particular customers, types of transaction etc.

Kredittilsynet emphasises that the measures implemented should include participation in special training programmes in which employees and other persons learn to recognise transactions which may be related to the laundering of proceeds of crime and terrorist financing, and receive instruction in how to proceed in such cases. All personnel in the

undertaking who deal with transactions, settlement and control functions must be informed of the identity of the undertaking's money laundering officer.

Svein-Henning Kjelsrud

Kjell Arne Aasgaarden

Contact persons:

Svein Hagen, tel. +47 22 93 99 12

Lene E. Andersen, tel. +47 22 93 99 16

Enclosure 1: Act on measures to combat the laundering of proceeds of crime etc., (No. 41 of 20 June 2003, Money Laundering Act)

Enclosure 2: Regulations on measures to combat the laundering of proceeds of crime etc., (No. 1487 of 10 December 2003, Money Laundering Regulations)

Enclosure 3: Annex 1 to the Consolidate Banking Directive (Directive 2000/12/EC of 20 March 2000)

Enclosure 4: Relevant forms posted on ØKOKRIM's website