Regulations relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering Regulations)

Chapter 1. Introductory provisions

Section 1-1 *Scope*

These Regulations apply to obliged entities within the meaning of the Anti-Money Laundering Act.

Section 1-2 *Agents of foreign payment service undertakings*

(1) Chapters 4 and 5 and Sections 40 and 52 of the Anti-Money Laundering Act apply to agents of payment service undertakings from other EEA states which are established in Norway.

(2) The Financial Supervisory Authority may supervise compliance with the provisions of paragraph 1 by agents of foreign payment service undertakings.

(3) The Financial Supervisory Authority may in the event of severe violations impose orders etc., pursuant to Section 47 of the Anti-Money Laundering Act. The Financial Supervisory Authority may in such cases also order the agents to temporarily suspend operations in Norway.

Section 1-3 *Application of the Anti-Money Laundering Act to virtual currency*

(1) Providers of exchange services between virtual currency and official currency are obliged entities within the meaning of the Anti-Money Laundering Act. This shall apply correspondingly to virtual currency custodianship services.

(2) By virtual currency is meant a digital expression of value, which is not issued by a central bank or a government authority, which is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but which is accepted as a means of exchange, and which can be transferred, stored or traded electronically.

(3) By virtual currency custodianship services is meant the custodianship of private cryptographic keys on behalf of customers, for purposes of transferring, storing or trading in virtual currency.

(4) The Financial Supervisory Authority may supervise compliance with the Anti-Money Laundering Act for the providers mentioned in paragraph 1. Providers as mentioned in paragraph 1, shall be registered with the Financial Supervisory Authority. The following information shall be registered on the provider:

a) name
b) type of enterprise and organisation number
c) business address
d) the service which is offered
e) name, residence address and personal identity number or D-number on
    1. the general manager or persons in a corresponding position
    2. members of the board of directors or persons in a corresponding position

3. any other contact person

Chapter 2. Maximum amount for cash payments

Chapter 3. Risk-based approach and procedures

Chapter 4. Customer due diligence measures and ongoing monitoring

Section 4-1 *Establishment of a customer relationship*

(1) A customer relationship shall be held to have been established when the customer can make use of the services of the obliged entity, for example upon the creation of an account or the issuance of a payment card.

(2) Government-authorised and registered auditors are held to have established a customer relationship when they have accepted an engagement, including advisory services and other services, or have sent an auditor's statement to the Register of Business Enterprises, cf. Section 4-4 of the Register of Business Enterprises Act.

(3) Authorised accountants are held to have established a customer relationship when they have concluded a written engagement agreement with a client or an engagement presupposes a written agreement, cf. Section 3 of the Accountants Act.

(4) Estate agents providing estate agency services are held to have established a customer relationship with a client when they have accepted a sale or purchase engagement. The first sentence applies correspondingly to cooperative building associations and lawyers providing estate agency services, when the engagement concerns such services.

(5) Lawyers and other persons who provide independent legal assistance on a professional or regular basis are held to have established a customer relationship when they have accepted an engagement as referred to in Section 4, Sub-section 2, letter c), of the Anti-Money Laundering Act. Lawyers and other persons who provide independent legal assistance on a professional or regular basis are in any event held to have accepted an engagement as referred to in the first sentence when an engagement confirmation is sent to the client.

Section 4-2 *Exemptions from the requirement for customer due diligence measures*

The duty to apply customer due diligence measures pursuant to Section 10, paragraph 1 letters a) and b) of the Anti-Money Laundering Act, is not applicable to

a) the establishment of non-life insurance policies, including travel insurance policies, and credit insurance policies; or
b) the issuance of electronic money, provided that
    1. the maximum amount that can be stored on the electronic medium is EUR 250 and the medium cannot be reloaded; or
    2. there is a limit of EUR 2 500 for the total amount transferred in a calendar year, unless the holder has redeemed an amount of no less than EUR 1 000 in the same calendar year.

Section 4-3 *Valid proof of identity for natural persons*

(1) Valid proof of identity for natural persons upon personal appearance is original versions of documents that

a) are issued by a government authority or another body that maintains adequate document issuance control procedures, which documents offer a satisfactory level of security;
b) include full name, signature, photograph; and
c) personal identity number or D-number.

(2) For persons who do not have a Norwegian personal identity number or D-number, the proof of identity document shall, in addition to the requirements laid down in paragraph 1, include the date of birth, the place of birth, the gender and the citizenship.

(3) The signature requirement does not apply to passports.

(4) Electronic signature is valid proof of identity for natural persons when identity shall not be verified upon personal appearance. Electronic signature shall comply with the requirements laid down in Section 3 of Regulations of 21 November 2005 No. 1296 relating to Voluntary Self-Declaration Arrangements for Certificate Issuers and be entered on a published list pursuant to Section 11, paragraph 1, of the said Regulations.

Section 4-4 *Customer due diligence measures for customers that are not natural persons and that are not yet registered in a public register. Subsequent obtaining of transcript or certificate of registration*

(1) For customers that are not natural persons and that are not yet registered in a Norwegian public register, obliged entities shall obtain documentation to the effect that the person exists and a written declaration from a natural person representing the customer to the effect that information obtained regarding the legal entity is correct.

(2) Upon the verification of information as outlined in Section 13 paragraph 2, first sentence, of the Anti-Money Laundering Act for a legal entity subject to a deadline for registration in a public register, the obliged entity shall obtain a transcript or certificate of registration from the public register within four weeks of the registration or the expiry of the deadline for registration.

Section 4-5 *Outsourcing to the distribution network of obliged entities and to providers of mailing services that are subject to a universal service obligation*

Outsourcing service providers performing services for or on behalf of an obliged entity when forming part of the distribution network of the obliged entity are regarded as part of the obliged entity within the meaning of Section 23 of the Anti-Money Laundering Act. The same applies to providers of mailing services that are subject to a universal service obligation. The outsourcing under the first and second sentences is limited to identity verification only, provided that the outsourcing service provider is not itself an obliged entity. The outsourcing is otherwise subject to the requirements in Section 23 of the Anti-Money Laundering Act.

Section 4-6 *Low risk of money laundering and terrorist financing – simplified customer due diligence measures*

(1) In situations in which the obliged entity finds that there is a low risk of money laundering and terrorist financing, the scope of customer due diligence measures may be reduced.

(2) In making such assessment, the following factors may give an indication that there is a lower risk of money laundering and terrorist financing:

a) Risk factors relating to the type of customer:
   1. companies listed on a regulated market that are subject to disclosure obligations which ensure adequate transparency of beneficial owners;
   2. public administrative bodies or companies; and
   3. customers that are resident in states held to entail lower risk.

b) Risk factors relating to the type of product, transaction, service provision or delivery channel:
   1. life insurance policies for which the annual premium is low;
   2. pension insurance policies that have no early surrender clause and that cannot be used as collateral;
   3. pension schemes or similar employee schemes, if contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
   4. limited financial products or services provided to certain customer groups for the purpose of promoting financial inclusion; and
   5. products where the risk of money laundering and terrorist financing is managed by other factors such as maximum amounts or transparency of ownership.

c) Geographical risk factors:
   1. EEA states;
   2. third countries identified as countries that have implemented satisfactory and effective measures to combat money laundering and terrorist financing; and
   3. third countries identified as countries having a low level of corruption and other criminal activity.

Section 4-7 *Simplified customer due diligence measures in respect of persons who have been granted a right of disposal and persons who can act on behalf of the customer*

When obliged entities may apply simplified customer due diligence measures pursuant to Section 16 of the Anti-Money Laundering Act, requirements for verification of the identity of persons who act on behalf of the customer or who have been granted a right of disposal over an account or a deposit may also be eased.

Section 4-8 *Customer due diligence measures in respect of accounts receiving funds from multiple persons (client accounts)*

Banks and credit institutions shall, for customers holding accounts with funds from multiple persons (client accounts), consider the customer's underlying clients to be beneficial owners of such accounts. Banks and credit institutions may nonetheless refrain from identifying and verifying the identity of beneficial owners of accounts referred to in the first sentence, provided that

a) the customer maintaining the account is subject to provisions on measures to combat money laundering and terrorist financing in conformity with international standards;
b) compliance with such requirements is supervised; and
c) information on the identity of beneficial owners is available to the bank or credit institution upon request.

Section 4-9 *High risk of money laundering and terrorist financing – enhanced customer due diligence measures*

In assessing whether there is a higher risk of money laundering or terrorist financing, cf. Sections 9 and 17 of the Anti-Money Laundering Act, the following factors may give an indication that the risk of money laundering and terrorist financing is high:

a) Risk factors relating to the type of customer:
    1. the customer relationship is conducted in unusual circumstances;
    2. customers are resident in areas held to entail higher risk, cf. letter c;
    3. legal entities or legal arrangements that are personal asset management companies;
    4. companies that have nominee shareholders or bearer shares;
    5. cash-based businesses; and
    6. companies whose ownership structure appears unusual or excessively complex given the nature of their business.
b) Risk factors relating to the type of product, transaction, service provision or delivery channel:
    1. private banking;
    2. products and transactions that favour anonymity;
    3. customer relationships or transactions established and performed without personal attendance, without making use of measures such as electronic signature;
    4. payments from unknown third parties; and
    5. new products and services, including new delivery mechanisms and the use of new technology in the development of new and pre-existing products.
c) Geographical risk factors:
    1. countries identified as countries that have not implemented satisfactory and effective measures to combat money laundering and terrorist financing;
    2. countries identified as countries having significant levels of corruption and other criminal activity;
    3. countries subject to sanctions, embargos or similar measures issued by the UN or the EU; and
    4. countries providing funding or support for terrorist activities or that have known terrorist organisations operating within their country.

Section 4-10 *Special measures in respect of high-risk countries*

(1) If a customer or beneficial owner is established in the following states, enhanced customer due diligence measures shall be applied:

a) Afghanistan
b) Bosnia & Herzegovina

c) Guyana
d) Irak
e) Lao PDR
f) Syria
g) Uganda
h) Vanuatu
i) Yemen
j) Etiopia
k) Sri Lanka
l) Trinidad & Tobago
m) Tunisia
n) Iran
o) Nord-Korea
p) Pakistan

(2) If a third party as referred to in Section 22 of the Anti-Money Laundering Act is established in a state mentioned in paragraph 1, the obliged entity cannot rely on customer due diligence measures performed by such third party.

Section 4-11 *Gathering information on the origin of the funds*

Obliged entities may gather information on the origin of the funds upon the implementation of customer due diligence measures, ongoing monitoring and further examinations, cf. Section 9 of the Anti-Money Laundering Act.

Section 4-12 *Use of third parties by providers of gambling services*

(1) Enterprises licensed to provide gambling services under the Gaming Scheme Act or the Parimutuel Betting Act may rely on customer due diligence measures performed by other enterprises licensed to provide gambling services under the Gaming Scheme Act or the Parimutuel Betting Act. Providers of gambling services licenced under the Lottery Act may rely on customer due diligence measures performed by enterprises licensed to provide gambling services under the Gaming Scheme Act or the Parimutuel Betting Act.

(2) Enterprises as referred to in paragraph 1 may, for gambling involving a joint prize pot with foreign providers of gambling services, refrain from applying customer due diligence measures to persons who have established a customer relationship or conducted a transaction with a foreign provider of gambling services. The first sentence shall only apply to cases in which the foreign provider of gambling services is in compliance with its home state's regulatory provisions on measures to combat money laundering and terrorist financing.

Chapter 5. Further examinations. Reporting

Section 5-1 *Submission of information to Økokrim*

(1) The person responsible for the submission of information to Økokrim [FIU] as referred to in Section 26 of the Anti-Money Laundering Act is the person designated as responsible pursuant to Section 8 paragraph 5 of the Anti-Money Laundering Act.

(2) The submission of information shall be effected electronically via Altinn. If this is not feasible, the submission of information may be effected by using a form developed by Økokrim.

Chapter 6. Processing of personal data and other information

Section 6-1 *Processing of sensitive personal data*

Obliged entities may process sensitive personal data when it is necessary to do so in order to comply with obligations under the Anti-Money Laundering Act or regulations issued pursuant to the Act.

Section 6-2 *Recording and retention of information and documents*

(1) The wording «true copy certified» shall be applied to copies of submitted proof of identity documents as referred to in Section 4-3 of the Anti-Money Laundering Regulations and Section 13 paragraph 2 of the Anti-Money Laundering Act, together with the signature of the person who has performed the verification, as well as the date of such verification. Instead of the signature and wording referred to in the first sentence one may otherwise ensure correspondingly reliable documentation of the verification, including who has performed the verification and when such verification was performed.

(2) Documents and information shall be retained on a medium that maintains the reading quality throughout the retention period.

(3) There shall be made a backup copy of electronic materials. The backup copy shall be retained separately from the original.

Section 6-3 *Retention of information and documents for lawyers, etc.*

Obliged entities as referred to in Section 4 paragraph 2 letter c), of the Anti-Money Laundering Act may retain information and documents falling within the scope of Section 30 of the Anti-Money Laundering Act for the duration of the client relationship, also where such information and documents have been obtained in connection with an individual transaction. The provisions of the Anti-Money Laundering Act shall otherwise apply to the processing of the information and documents.

Section 6-4 *Calculation of maximum retention period*

The overall retention period under Section 30 paragraph 4 of the Anti-Money Laundering Act shall be calculated from the termination of the customer relationship or the completion of the transaction.

Section 6-5 *Intragroup exchange of information*

(1) Information may be exchanged, irrespective of any duty of confidentiality, between group companies referred to in Section 31 paragraph 1 of the Anti-Money Laundering Act, as part of measures to combat money laundering and terrorist financing when such information concerns:

a) a joint customer; or
b) customers having a special affiliation with each other, for example an affiliation indicating a joint beneficial owner, or in other circumstances which may suggest that a transaction or activity is conducted on behalf of the same person.

(2) The information that may be exchanged includes all relevant information and documents obtained or prepared pursuant to the Anti-Money Laundering Act and appurtenant regulations, including information on the customer, beneficial owners, accounts, transactions, etc. A joint customer register may be used to determine whether the exchange of information pursuant to the present provision is permitted.

(3) The exchange of such information may also take place upon the establishment of a customer relationship.

(4) The scope for receiving information from other group companies will not affect the enterprise's own responsibility for risk classification, customer due diligence measures, etc., under the anti-money laundering provisions.

(5) The group shall have a centralised function for information sharing under the present provision, for purposes of handling the group's risk of money laundering and terrorist financing. The centralised function shall for such purposes be granted access to all information falling within the scope of this provision. As far as branches and subsidiaries of foreign enterprises are concerned, the requirement for a centralised function applies to the Norwegian part of the business, provided that the home state's anti-money laundering provisions do not require the establishment of a corresponding centralised function.

Chapter 7. Miscellaneous obligations

Section 7-1 *Establishment of a national contact point*

(1) Foreign payment service undertakings with agent activities in Norway shall appoint a national contact point when

a) the undertaking has ten agents or more in Norway;
b) the aggregate payment transactions of the undertaking exceed, or are expected to exceed, an amount corresponding to EUR 3 million per financial year; or
c) the undertaking fails to disclose to the Financial Supervisory Authority the information needed to assess whether letter a) or b) is applicable.

(2) The Financial Supervisory Authority may in special cases order foreign payment service undertakings to appoint a national contact point when there is reasonable cause for assuming that there is a high risk of money laundering and terrorist financing associated with the agent activities of such undertakings.

(3) The Financial Supervisory Authority may order the temporary suspension of the operations of the undertaking in Norway until a national contact point has been appointed.

Section 7-2 *The duties of national contact points*

(1) The national contact point shall ensure that the agents are complying with Norwegian anti-money laundering provisions.

(2) The national contact point shall in relation to the Financial Supervisory Authority

a) represent the affiliated agent;
b) provide access to information held by the agent; and
c) facilitate supervision of the agents.

(3) The national contact point shall conduct enquiries, report to Økokrim [FIU] on behalf of the agents and submit information to Økokrim [FIU] on behalf of the agents, cf. Sections 25 and 26 of the Anti-Money Laundering Act. The Financial Supervisory Authority may grant exemptions from the duty of national contact points to conduct enquiries in cases in which this is otherwise handled satisfactory by the foreign payment service undertaking.

(4) The national contact point shall be located in Norway and have a good knowledge of the Norwegian language and Norwegian anti-money laundering provisions.

(5) The Financial Supervisory Authority may upon violation of the duties under paragraph 2 issue a cease and desist order and levy a coercive fine pursuant to Section 47 of the Anti-Money Laundering Act.

Chapter 8. Authorisation for company service providers

Chapter 9. Supervision. Administrative measures. Sanctions

Chapter 10. Concluding provisions

Section 10-1 *Information that shall accompany a payment*

The EEA Agreement Appendix IX no. 23d (Regulation (EC) no. 1786/2006) on information on the payer which shall accompany a payment, applies as regulations with the adjustments that follow from Appendix IX, Protocol 1 to the Agreement and the Agreement as a whole.

Section 10-2 *Transitional provisions*

(1) Payment service undertakings that are subject to the duty to appoint a national contact point shall notify the Financial Supervisory Authority of the national contact point within three months of entry into force of these regulations.

(2) Providers of exchange or custodianship services as mentioned in Section 1-3 paragraph 1, shall register with the Financial Supervisory Authority in accordance with Section 1-3 paragraph 4 within three months of entry into force of these regulations.

Section 10-3 *Entry into force*

(1) These Regulations shall enter into force on the 15th of October 2018.

(2) From the time of entry into force, Regulations of the 13th of March 2009 no. 302 on Measures to Combat Money Laundering and Terrorist Financing etc. and Regulations of the 13th of March 2009 no. 303 on the Supervisory Board for Measures to Combat Money Laundering are repealed.