CLIFFORD
CHANCE

Client Briefing
October 2008

Financial Services Client Briefing

The Dutch Implementation of the Third Money Laundering Directive; The Prevention of Money-Laundering and Terrorist Financing Act

Contents

The Dutch landscape of integrity legislation was until recently substantially formed by the Customer Identification Act (*Wet identificatie dienstverlening*, the "**WID**") and the Unusual Transaction Reporting Act (*Wet melding ongebruikelijke transacties*, the "**MOT**"). The regulatory landscape underwent some noteworthy reshaping as a consequence of the implementation of the Third Money Laundering Directive (2005/60/EC, the "**Directive**").

The WID and the MOT were first aligned, then amended by the implementation of the Directive and subsequently combined in the new Prevention of Money-Laundering and Terrorist Financing Act (*Wet ter voorkoming van witwassen en de financiering van terrorisme*, the "**Act**"). Contrary to the rule-based approach of the WID and the MOT, the Act takes a principles based approach.

Despite the implementation deadline of 15 December 2007, which was met by most EU countries, the Act came into force in the Netherlands on 1 August 2008. This briefing addresses the requirements introduced by the Act and its consequences for market parties.

The Directive

In principle, the Act mirrors the Directive in its provisions. The Directive aims to bring EU legislation in line with the revised Recommendations published by the Financial Action Task Force (the international body responsible for setting standards and developing policies to combat money laundering and terrorist financing) and to improve anti money-laundering procedures generally.

The Directive clarifies the customer identification procedures in respect of (legal) persons, *i.e.* the inquiry into their identity and background. This inquiry is defined in the Directive as Customer Due Diligence ("**CDD**") and includes, for example, the identification of the ultimate beneficiary in certain transactions or business relationships and an analysis of the structure of the group which a legal person is part of.

Furthermore, the Directive enables the possibility to apply CDD measures proportionally to the risk that a certain customer, relationship or business transaction entails in terms of money laundering or terrorist financing.

If you would like to know more about the subjects covered in this publication or our services, please contact:

Frank Graaf, + 31 (0)20 711 9150
Frank.Graaf@cliffordchance.com

Rezah Stegeman, + 31 (0)20 711 9116
Rezah.Stegeman@cliffordchance.com

Joost van Hout, + 31 (0)20 711 9232
Joost.vanHout@cliffordchance.com

Wouter van den Berg, + 31 (0)20 711 9166
Wouter.vandenBerg@cliffordchance.com

Clifford Chance LLP, Droogbak 1A,
1013 GE Amsterdam, The Netherlands

www.cliffordchance.com

The main changes introduced under the Act

Addressees

- Institution-based

In contrast to the WID, in which conducting certain services triggered its applicability, the Act is "institution-based". This means that the applicability of the Act is not triggered by a specified *service*, but becomes applicable if a specified *institution* establishes a business relationship or carries out a certain transaction with a customer. The list of institutions includes financial undertakings (*financiële ondernemingen*) such as banks, life insurers, investment firms and investment institutions. In addition, the list includes non-financial institutions such as tax advisers, accountants, casinos and lawyers. Contrary to the WID, the Act covers "Annex I" businesses (*financiële instellingen*) which are businesses that conduct activities listed in Annex I of the Banking Consolidation Directive (2006/48/EC). These activities include, among others: (i) lending, (ii) financial leasing, (iii) safe custody services and (iv) issuing and administering means of payment (e.g. credit cards). Consequently, any otherwise unregulated businesses that carry on such activities are, in principle, subject to the Act's provisions.

- Branches and cross-border business

Branches and subsidiaries *in the Netherlands* of foreign financial undertakings are also subject to CDD requirements under the Act. Further, the Act requires non-EU branches and subsidiaries of Dutch financial undertakings *outside the Netherlands* to have equivalent CDD procedures in place too.

Customer Due Diligence

The most significant feature introduced by the Act is the concept of CDD, which is much broader than identification under the WID as it also requires, for example, the identification of the ultimate beneficiary and an inquiry into the purpose of the relationship. Institutions within the scope of the Act are obliged to apply CDD whenever they establish business relationships, carry out certain transactions or if there are indications that a customer is involved in money laundering or terrorist financing.

Dutch banks and life insurers are already familiar with CDD obligations similar to those set out in the Act, since they are subject to the Prudential Rules Decree FSA (*Besluit prudentiële regels Wft*). However, for other institutions the concept of CDD will be relatively new.

Risk-based approach

The Act introduces a three-tiered risk-based approach, dependent on the level of the money laundering or terrorist financing risk presented by the customer. The three levels of CDD are: standard, simplified and enhanced.

- Standard CDD

Standard CDD applies in all cases unless simplified CDD (see below) applies. It must be applied in such a manner to enable the institution to:

(a) identify the customer and verify its identity;

(b) identify, where applicable, the ultimate beneficiary and verify its identity;

(c) identify the purpose and intended nature of the relationship; and

(d) to the extent possible, conduct ongoing monitoring of the business relationship and of transactions undertaken throughout the course of that relationship;

Re (a) Identification of the customer

The identity of a client must be verified with documents, data or information from a reliable and independent source. The following documents will suffice:

i. for Dutch and foreign individuals (natural persons): passports, identification cards or driver's licences. This is not an exhaustive list and other reliable documents may suffice as well.

ii. for legal entities that have their registered office in the Netherlands: the certified copy of registration with the relevant Chamber of Commerce. Contrary to the WID, this now includes online certified extracts, which are easily obtainable. Other reliable documents, such as a deed from a civil notary, would also suffice.

iii. for legal entities that have their registered office outside the Netherlands, identity is verified using reliable documents that are customarily used in international business or are recognised under the law of the relevant state.

Re (b) Ultimate beneficiary

The standard CDD measures under the Act include the identification and verification of so-called ultimate beneficiaries, a requirement that did not exist under the WID. In short, any person who controls at least 25% of a company or partnership, or who otherwise exercises control over the management of such a body, should be regarded as an ultimate beneficiary. In the context of trusts and foundations an ultimate beneficiary is a beneficiary of 25 % or more of the capital or a person who has particular control over 25 % or more of the capital of a trust or foundation.

Re (d) Ongoing monitoring

Transaction monitoring is a mandatory requirement under the Act. Institutions must monitor business relationships on an ongoing basis and regularly update the CDD information that they hold. Furthermore, an institution must ensure that the transactions carried out during the relationship are consistent with the information the institution holds on the customer and its risk profile. As a result, an interim inquiry into the source of funds may be necessary. Contrary to the WID, if the customer itself has been identified by the institution, the Act does not explicitly require all such customer's representatives (that the institution deals with during the course of the business relationship or transaction) to be identified.

- Simplified CDD

Simplified CDD is applicable instead of standard CDD where the customer falls within various categories specified in the Act that have limited susceptibility to money laundering. These categories include banks and financial undertakings that are subject to the Act and institutions that are listed on a stock exchange.

- Enhanced CDD

Enhanced CDD measures must be applied on a risk-sensitive basis in certain situations which are deemed to present a higher risk under the Act. These situations include (i) where a bank has a correspondent banking relationship with a bank from a non-EEA state, (ii) where the customer is a politically exposed person (PEP) or is not physically present for identification purposes, and (iii) any other situation which due to its nature can present a higher risk of money laundering or terrorist financing.

Reliance on third parties

If customers are introduced to an institution by third parties, it may rely on those third parties to meet the CDD requirements, provided that the third parties are institutions based in the EEA and subject to equivalent CDD requirements. However, the third parties must provide the data and documents regarding the identity of the customer or ultimate beneficiary to the institution.

Apart from the above, 'derived identification', a concept already known under the WID, can still be applied under the Act if a customer is not physically present. In such a situation, an institution may rely on CDD measures performed by a bank based in the EEA, if the first payment relating to a certain set of transactions is carried out through an account opened in the customer's name with that bank.

Finally, outsourcing of CDD is also possible under the Act. In certain circumstances, an institution may rely on third parties conducting CDD measures on its behalf. However, the relevant institution will remain responsible for any failure in applying CDD measures properly.

Reporting of unusual transactions: no significant changes

The rules regarding the reporting of unusual transactions have not materially changed. The most important difference relates to the change of addressees (institutions as referred to above instead of just anyone).

Institutions must notify an effected or intended unusual transaction within 14 days after the unusual nature of the transaction has become known. A transaction is considered to be unusual by reference to certain indicators. One "subjective indicator" and several "objective indicators" have been formulated. The subjective indicator requires a personal assessment by the institution and states that if the institution suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being, or has been committed or attempted, the transaction should be considered unusual. Examples of the objective indicators are cash transactions over EUR 15,000 and transactions with (legal) persons established in designated countries or territories. These situations should always be considered unusual.

Supervision and enforcement

The Dutch financial regulators, in addition to their usual roles, supervise compliance with the Act. Either the Dutch Financial Markets Authority (*Stichting Authoriteit Financiële Markten*, the "**AFM**") or the Dutch Central Bank (*De Nederlandsche Bank*, "**DNB**") exercises such supervision over financial undertakings such as banks, investment firms or investment institutions.

A breach of the Act could result in the imposition of an order to cease and desist or result in a fine up to a maximum of EUR 32,670.

On 14 August 2008, DNB and the AFM informed the market that institutions may rely on a grace period until 1 January 2009 to amend their policies to conform to the Act's new provisions. Enforcement of the Act will only start after this date. Until then, the WID and the MOT provisions still apply and will be enforced. ■