BRANDSTÄTTER RECHTSANWÄLTE GMBH

DR. JÜRGEN BRANDSTÄTTER
VICTORIA ROSENGREN, LL.M.(RAK-Berlin)

WALLNERSTRASSE 3 · A-1010 WIEN
TEL: +43.1.535 16 30
FAX:+43.1.535 16 30-40

OFFICE@BMA-LAW.COM
WWW.BMA-LAW.COM

Money Laundering – who cares?

By Dr. Jürgen Brandstätter,
BMA Brandstätter Rechtsanwälte GmbH

The short answer to this matter is „YOU“, or at least you should.

Just to give you two examples how sensitive the issue is:

The former presidential candidate **Bob Dole** was once under investigation for money laundering for carrying too much cash in his pockets. During the investigation he testified that he paid cash since his war injury, a paralyzed right arm, made it difficult for him to pay otherwise. Investigations were eventually dropped.

Many years later, a bank clerk informed authorities that Mr. **Eliot Spitzer**, Governor of the State of New York, was withdrawing cash on a regular basis which then led to investigations which uncovered his regular visits to hookers and the like. He later stepped down as governor.

Hence, money laundering is a sensitive issue which can lead to your being investigated or publicly embarrassed. While I will not talk about the undoubtedly harmful effects of money laundering, I will talk of the rules and regulations which might affect your business.

The long answer is therefore the European Union Money Laundering Directive and its many implications for your business. There are also two UN Conventions (UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, UN Convention Against Transnational Organized Crime of 2001 and UN Convention Against Corruption of 2005) regarding money laundering. But since they basically cover the same ground we will focus today on the European Union Money Laundering Directive.

SITZ IN WIEN
FN 275004 v HG Wien

BANKVERBINDUNG:
PSK, BLZ 60000
KONTO NR. 92.179.437
BIC: OPSKATWW
IBAN: AT226000000092179437

UID-NR. ATU 62356612
DVR 3000455

Background:

In 1989, the G7 founded the Financial Action Task Force on Money Laundering (FATF), as an intergovernmental organization housed at the OECD headquarters in Paris. The purpose of the FATF is to develop policies to combat money laundering and terrorism financing. Recommendations made by the FATF are then transformed into EU law.

The First Money Laundering Directive (91/308/EEC) concentrated on combating the laundering of drugs proceeds through the traditional financial sector. This imposed obligations on financial sector firms, which included requirements relating to maintaining systems for customer identification, staff training, record keeping, and reporting suspicious transactions.

The Second Money Laundering Directive (2001/97/EC) amended the 1991 Directive to introduce changes in two main areas:

- It expanded the scope of predicate offences for which suspicious transaction reporting was mandatory, from drug trafficking to all serious offences; and
- It extended the scope of the Directive to a number of non-financial activities and professions (including lawyers, notaries, accountants, estate agents, art dealers, jewelers, auctioneers and casinos).

The Third Money Laundering Directive (2005/60/EC), of which I will speak today reflects the 2003 recommendations of the FATF, namely the risk based approach of which I will come to speak later. It replaces the First Money Laundering Directive as amended by the Second Money Laundering Directive.

The act applies to the following professionals:

- Credit institutions as well as financial institutions
- Auditors, insolvency practitioners, external accountants and tax advisors
- Independent legal professionals (does not include in-house counsel)
- Trust or company service providers
- Estate agents
- High value dealers
- Casinos

Activities covered by the regulation:

- Buying and selling of real property or business entities
- Managing of client money, security or other assets
- Opening or management of bank, savings or securities accounts

- Organization of contribution necessary for the creation, operation or management of companies
- Creating, operation or management of trusts, companies or similar structures.

Activities not covered by the money laundering directive:

- Preparing a home information pack or any document or information for inclusion in a HIP
- Payment on account of costs to a solicitor or payment of a solicitor's bill
- Provision of legal advice
- Participation in litigation or a form of alternative dispute resolution
- Will-writing, although accompanying taxation advice could be covered.

Risk based approach:

Since the above mentioned criteria would cover a lot of completely harmless transactions, the third Money Laundering Directive has introduced the so called risk based approach. Once a transaction and/or client is identified as falling under the Money Laundering Directive, the parties involved have to determine the risk of actual money laundering and the appropriate checks and balances. The need for a risk based approach is best illustrated in my first example of a presidential candidate with a lot of cash who is obviously not a money laundering risk.

Clients with potential higher risk:

- Politically exposed Persons (PEPs), near family member and people closely associated to them
- Large and implausible distances between the company and the clients domicile
- Moving of accounts without explanation
- Moving of assets between different company branches without explanation
- Unusual cash withdrawals
- Use of elaborate company structures ("off-shore") where the owner is not obvious
- Moving of assets not in accordance with the business idea behind the transaction
- Etc…

Certain products offered by banks are assumed to be high risk:

- Private banking when large sums are involved.
- Off-shore companies, trusts etc. where the owner is not obvious.
- Cross border banking relations with third countries are deemed to be high risk by law
- Services where there is no personal contact with the client such as:

    - Online banking
    - Electronic money transfer and credit card payment
    - New technologies
    - Business contact through the internet
    - Use of ATM/cash machines to get or deposit money
    - Orders per fax or e-mail
- Credit settlements
- Financing of high risk goods to countries subject to embargos
- Savings deposits not under the clients name where the beneficiary might make transactions using a code word
- Cash businesses
- Non-resident accounts, number accounts, clients where the correspondence is picked up at the branch.

Larger companies/firms should consider making their risk assessment in writing so it may be presented to authorities.

Customer Due Diligence (CDD):

Assuming there is a risk, **Customer/Clients Due Diligence (CDD)** has to be conducted when:

- Establishing a business relationship
- Carrying out an occasional transaction
- Money laundering or terrorist financing is suspected
- Veracity or adequacy of documents, data or information previously acquired for the purpose of CDD is questioned

Measures to be taken are determined according to the previously determined risk:

- Information to be recorded (to be kept for five years)
    - Identifying customer
    - Identifying, where applicable, the beneficial owner
    - Obtaining information on the purpose and intended nature of the business relationship
    - Conducting ongoing monitoring, on a risk sensitive basis
- Information to be obtained to verify identity from an independent source (in case of higher risk clients)
- Whether simplified due diligence may occur (e.g. where client is a bank from a member state)
- Whether steps need to be taken for enhanced due diligence

- What steps need to be taken for enhanced due diligence
- What steps need to be taken to ascertain whether client is a PEP
- At what point CDD need to occur and under what circumstances delayed CDD is permitted
- How to conduct CDD on existing clients
- What ongoing monitoring is required

Attention: These measures have to be applied to existing clients also.

Consequences:

Where the identification requirements cannot be met the business relationship should not be established or terminated, or the transaction should not be undertaken. A report has to be filed with the member states Financial Intelligence Unit. The client/customer will not be informed of this in order not to jeopardize investigations.

Conclusion:

Lawyers, banks and others falling under the directive therefore have to check how these directives have been transformed into national law and to develop a system to meet the due diligence obligations and establish a client risk profile in a risk based and proportionate manner. Policies and procedures supporting these systems mean that staff applies the system consistently and firms can demonstrate to oversight bodies that compliance measures are in place.

For companies, it is vital to provide the financial institutions with sufficient information. Keeping in mind that they are obligated to inform authorities in a number of cases, it is advisable to have a close working relationship where the bank is informed of transactions in advance and later updated. The same of course applies to lawyers, tax advisors and others. A transaction which might appear harmless to you, not fully explained, might otherwise trigger a number of consequences.

Vienna, October 2012