(COP 10) MONEY LAUNDERING AND FINANCE OF TERRORISM

A *Definitions and applicability*

Beneficial owner is the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Money laundering is the process by which the financial proceeds of crime are disguised to conceal their illegal origin.

The **financing of terrorism** is any kind of financial support to those who encourage, plan or engage in terrorism. The meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country.

Know Your Customer (KYC) principles are principles established to combat money laundering and finance of terrorism. KYC principles require businesses to establish the identity of all organisations with which they deal, have a clear understanding of their business relationships and have a reasonable ability to identify and react to transaction patterns appearing out of the ordinary or suspicious.

Source:

- *World Bank – Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* *http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf*
- *Financial Action Task Force – RBA Guidance for Dealers in Precious Metal and Stones* *www.fatf-gafi.org/documents/riskbasedapproach/fatfguidanceontherisk-basedapproachfordealersinpreciousmetalsandstones.html*

The Money Laundering and Finance of Terrorism section of the COP is applicable to all Facilities.

B *Issue background*

Money laundering is the term for a multitude of practices designed to hide illegal or 'dirty' money. The profits from criminal activities – such as illegal arms sales, drug trafficking, prostitution, fraud, insider trading, theft or tax evasion – go through a succession of transfers and deals until the illegal source of the funds is obscured. The money then takes on the appearance of legitimate or 'clean' funds or assets.

The money laundering process usually follows three stages. In the initial – or placement – stage of money laundering, the launderer introduces the illegal profits into the financial system. This is often done by breaking up large amounts of cash into smaller sums. These are then deposited as cash, cheques or money orders directly into bank accounts in various locations.

After the funds have entered the financial system, the second – or layering – stage takes place. In this stage, a series of conversions or movements of the funds are carried out to distance them from their illegal source. The funds might be channelled through the purchase and sales of investments, or wired through a series of international bank accounts. This use of widely scattered accounts is especially prevalent in jurisdictions that do not co-operate in anti-money laundering investigations.

In the third stage – integration – the funds re-enter the legitimate economy. Legitimate and illicit proceeds may be commingled in the accounts of trading companies. The launderer might choose high value assets or goods for purchase and perhaps resale. These items can include real estate, business ventures, or products such as such as precious metals, diamonds, jewellery, cars or antiques.

Terrorist financing uses similar kinds of transactions for concealment and disguise, but with differences in stages one and three. In the first stage, funds for terrorist financing may originate from legitimate sources as well as criminal activities. Legitimate sources may include donations to foundations or charities that are in turn used to support terrorist activities or organisations. In the third stage, the distribution of funds is toward illegal organisations or their activities, while money laundering goes in the opposite direction – integrating criminal funds into the legitimate economy.

B *Issue background (cont)*

Money laundering and the financing of terrorism can, and do, occur in any country in the world. As dealers in high value goods, various parts of the jewellery supply chain may be targeted during the process of laundering money. It is therefore vital that the sector adopts very strict systems to minimize the risk of becoming involved in money laundering or terrorism financing.

C *Key regulations*

INTERNATIONAL STANDARDS

To co-ordinate an international response to money laundering, the Financial Action Task Force on money laundering (FATF) was established by the G-7 Summit in Paris in 1989. In 2001, the FATF mission was expanded to include reducing or eliminating the financing of terrorism.

The 2012 FATF Recommendations set out the measures which national governments should take to implement programs for preventing, detecting and suppressing both money laundering and terrorist financing, as well as other types of financial crime. The FATF has also issued a guidance document for a risk-based approach to combating money laundering and terrorist financing, designed specifically for dealers in precious metal and stones.

NATIONAL LAW

Most countries have enacted strict anti-money laundering legislation and regulations. Because of the criminal nature of the activity, it is essential to be aware of the relevant legislation in every operating jurisdiction. Dealing in high value goods, such as precious metals, stones or jewels, often triggers regulatory requirements to implement internal transaction monitoring and controls.

In the case of no national law, RJC requires Members to monitor and maintain records of all cash transactions equal to or above 15,000 Euro/US Dollars, where the transaction is carried out in a single operation or in several operations that appear to be linked. Members, when engaged in international transactions that may be subject to more than one regulatory jurisdiction, need to be aware of and comply with the Applicable Law for all relevant jurisdictions.

D *Suggested implementation approach*

The Suggested implementation approach provides general guidance for implementing the mandatory requirements of the Code of Practices. The guidance is not normative and should be seen as a starting point for information and support.

COP 10.1: KNOW YOUR CUSTOMER PRINCIPLES:

Members shall apply Know Your Customer principles for Business Partners that are suppliers or customers of Diamonds, Gold and Platinum Group Metals or Jewellery Products containing these, including:

a. **Establishing the identity, and where triggered by a Risk Assessment or Applicable Law, the beneficial ownership and principals of the supplier or customer;**

b. **Maintaining an understanding of the nature of their business;**

c. **Monitoring transactions for unusual or suspicious activity and reporting suspicions of money laundering or finance of terrorism to the relevant designated authority.**

D *Suggested implementation approach (cont)*

Points to consider:

- Business Partners do not include end consumers.
- Members should ensure they are aware of the Applicable Law for all relevant jurisdictions.
- A risk assessment should be carried out for the business to identify vulnerability to involvement in money laundering or the finance of terrorism. High risk indicators or 'red flags' should be established for screening of new customers or suppliers prior to initial transactions, and for ongoing monitoring of transactions.
- Higher-risk suppliers or customers would include those who show any of the following characteristics (see the FATF Guidance on the Risk-Based Approach for additional information):
  - Lack of knowledge of the industry
  - Requests for unusual financial terms and conditions
  - Lack of an established place of business, or an unusual location
  - Proposing a transaction that makes no sense
  - Use of banks that are unusual or distant
  - Use of non-bank financial institutions for no apparent legitimate business purpose
  - Frequent and unexplained changes in bank accounts
  - Frequent and unexplained changes in accounting personnel
  - Use of companies that do seem to have any legitimate fiscal, legal or commercial reason to be used
  - Unusually complex organizational structure
  - Offices located in higher risk jurisdictions
  - Involvement of third parties in transactions
  - Refusal to identify beneficial owners or controlling interests, where this would be commercially expected
  - Seeking of anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries
  - Use of cash in a nonstandard manner
  - Involve politically exposed persons.
- KYC procedures should be in place for establishing identity, and also the beneficial owners and principals of customers and/or suppliers (sometimes also called counterparties) where required by Applicable Law and/or where warranted based on the risk assessment.
  - Provide training for relevant employees on Know Your Customer and related compliance procedures, including relevant risk indicators.
  - Seek and maintain up to date records that document identification and awareness of the business for all relevant customers and suppliers.
  - The level of monitoring should be commensurate with the level of risk. Increased monitoring and tighter controls and approval authorities should apply for any customers or suppliers that are deemed higher risk, based on the risk assessment.
  - Establish procedures to identify and properly report suspicious activity to the appropriate authorities. If risks of money laundering or terrorism financing are identified, it is not the responsibility of Members to determine the type of underlying criminal activity, or intended terrorist purpose. The obligation is to identify and report the suspicious activity to the proper authorities. Reporting may be triggered as a result of a risk assessment, or through reporting rules that are set out in legislation.
- For larger businesses or those exposed to high risks, a formal anti-money laundering/counter-terrorist financing (AML/CFT) program should be established under the authority of a designated manager. It may be appropriate to implement the program in coordination with other business compliance and security programs. Consider engaging an independent qualified auditor to regularly review and test the AMC/CFT program and procedures.

D *Suggested implementation approach (cont)*

COP 10.2: CASH TRANSACTIONS:

Members shall maintain records of all cash or cash-like transactions which occur above the relevant defined financial threshold under Applicable Law and, where required, report these to the relevant designated authority. Where no Applicable Law exists, Members shall monitor and maintain records of all cash transactions equal to or above 15,000 Euro/US Dollars, where the transaction is carried out in a single operation or in several operations that appear to be linked.

Points to consider:

- The circumstances that will trigger a requirement to report a suspicious transaction or activity to a dealer's competent authority are usually rules-based and set forth in national law. It may include both business partners (B2B) and end consumers (B2C).
- Members should be aware of the relevant thresholds in all jurisdictions where they operate. Where no Applicable Law exists, the cash threshold for recording a transaction is at or above 15,000 Euro/US Dollars.
- Procedures should be in place that can automatically trigger a reporting requirement when the thresholds are exceeded.
- Transactions that are or appear to be linked should be considered a single transaction.

Q&A: MONEY LAUNDERING AND FINANCE OF TERRORISM

1. What happens if we seek identity information from customers or suppliers, but we don't receive it for everyone, despite chasing? Does our conformance rating rest on how our system and procedures work or achievement of 100% data?

The COP requires Members to establish the identity of all customers and suppliers, and where triggered by a risk assessment or Applicable Law, the beneficial ownership and principals of the supplier or customer. This does not necessarily mean '100% data' at all times as the collection and maintenance of relevant data is an ongoing process. Auditors should take into consideration the extent and nature of any missing information, the reasons why the information is missing, and whether it demonstrates weaknesses in the Member's management systems.

For example, there could at times be reasonable, practical reasons for certain identity information to be missing, such as information about a company that is out of date because the business relationship is inactive, or due to a move or a change of a phone number, or to a minor clerical error. However if basic identity information is missing such that an active counterparty could not be contacted or located, or there are frequent information gaps that indicate systems are not performing properly, then the Member is likely to be in a situation of non-conformance.

Gathering information about beneficial owners may not be as straightforward as basic identity information. For example, the results of a risk assessment may cause a Member to request information about beneficial ownership, but it may not be legally required, and the counterparty may not be cooperative, or the information may need to be 'chased' for a new customer, or for one that has recently changed ownership. However if information is legally required and missing, particularly for several accounts, or the Member is not able to demonstrate that it is taking action to gather the necessary information, then the Member is likely to be in a situation of non-conformance.

D *Suggested implementation approach (cont)*

Q&A: MONEY LAUNDERING AND FINANCE OF TERRORISM (CONT)

2. How can small business get information from very large companies?

Publicly available resources can sometimes provide access to relevant information. For example, Members may not need to recreate or verify counterparty information if the counterparty is already registered under a regulatory program and/or industry association that requires similar information. This includes, for example, members of bourses that are members of the World Federation of Diamond Bourses, companies listed on the Officially Registered Belgian Diamond Companies website, or member companies of the LBMA [Source: FATF - RBA Guidance for Dealers in Precious Metal and Stones.] There may also be exemptions under some national law for identification of beneficial owners of listed companies and financial institutions.

There are also some sectoral initiatives to support Know Your Customer approaches. For example in the Belgian diamond sector, the AWDC and the Federal Public Service Economy have collaborated to create a website tool for KYC: http://www.registereddiamondcompanies.be/

3. Is there a list of financial reporting thresholds by country?

The FATF Recommendations are the primary driver for financial reporting legislation in individual countries. There are currently over 180 jurisdictions that have committed to the FATF Recommendations via membership of the FATF or FATF-style regional bodies. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR15,000. Some countries will use the same threshold, while other countries may have lowered that threshold to a lower amount.

CHECK:

- Have you documented the identity of all business partners that are suppliers or customers of diamonds, gold and platinum group metals or jewellery products containing these?
- Have you carried out a risk assessment of these business partners to identify vulnerability to involvement in money laundering or the finance of terrorism?
- For high-risk suppliers and customers, or where required by regulation, have you established the beneficial ownership and principals of these businesses?
- Can you show the auditor how you monitor transactions for unusual or suspicious activity, against a general knowledge of the nature of their business?
- Do you have procedures for reporting suspicious transactions to the relevant designated authorities?

E *Further information*

The following websites have further information on anti-money laundering and combating the financing of terrorism:

- Basel Committee on Banking Supervision
  www.bis.org/bcbs/index.htm
- Deloitte - Audit of statutory financial statements (Belgium)
  www.deloitte.com/view/en_BE/be/services/aers/audit/auditrequirementsinbelgium/audit-of-statutory-financial-statements/index.htm
- Dube – Cuttini – Financial Statements
  http://dubecuttini.com/services/financial-statements/
- Financial Action Task Force (FATF)
  www.fatf-gafi.org
- FATF Recommendations – 2012
  www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
- FATF – RBA Guidance for Dealers in Precious Metals and Stones
  www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20Dealers%20in%20Precious%20Metal%20and%20Stones.pdf
- FATF Mutual Evaluations, by country
  http://www.fatf-gafi.org/topics/mutualevaluations/
- International Money Laundering Information Network (IMoLIN)
  www.imolin.org/imolin/index.html
- Jeweler's Vigilance Committee (US)
  www.jvclegal.org/
- Officially Registered Belgian Diamond Companies – A Tool for Know Your Customer
  http://www.registereddiamondcompanies.be/
- United Nations Office on Drugs and Crime (UNODC) - The Law Enforcement, Organized Crime and Anti-Money-Laundering Unit
  www.unodc.org/unodc/en/money-laundering/index.html
- World Bank Group – Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism (2006)
  http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf