Beck & Pollitzer

Anti-Money Laundering and Counter Terrorism Policy

Anti-Money Laundering and Counter Terrorism Policy

Scope

This policy applies to all employees, directors, officers, committee members, consultants, contractors, volunteers, interns, casual workers and agency workers of Beck & Pollitzer Limited and its subsidiaries (the "Company") .

Objective

The objective of this policy is to protect the Company, its people and its reputation from the risks associated with money laundering and terrorist activity through the application of anti-money laundering and counter terrorist financing procedures.

By following the procedures set out in this document, the Company can take steps to ensure that it is not used for illicit purposes and can protect its resources and reputation. The Company's key money laundering and terrorist financing risks will be related to operating transactions; however, they can arise in relation to any funds received by the Company. This policy refers to transactions below; but, applies equally to any type of funds that may be received.

The Policy

The Company will not allow itself to be used to launder proceeds from criminal activities. The Company recognises the need to have in place up to date procedures aiming to prevent money laundering.

All of the Company's activities will be managed in full compliance with this policy and the procedures outlined within it. This includes obligations to:

(a) ensure that the Company does not assist in laundering the proceeds of crime;

(b) report any knowledge or suspicion that the Company is being used for money laundering or terrorist financing purposes to the Group Legal Counsel; and

(c) conduct ongoing monitoring of the relationship with existing customers and of transactions.

The Company will comply fully with all applicable legal and regulatory obligations.

Failure to comply with this policy is a disciplinary offence which could result in disciplinary action. Moreover, it could constitute a criminal offence which could result in your prosecution.

Money Laundering

What is Money Laundering?

Money laundering is the process whereby criminals seek to conceal the true origin and ownership of the proceeds of their crime in order to give the impression that these proceeds originated from a legitimate source.

There are essentially three stages in money laundering:

(a) Placement: the physical disposal of criminal proceeds where the money launderer attempts to place cash into the financial system.

(b) Layering: the separation of criminal proceeds from their source by the creation of "layers" or a sequence of transactions designed to disguise the audit trail and provide the appearance of legitimacy.

(c) Integration: the conversion of the criminal proceeds, for example, into real estate, property or investments, so that they appear to be legitimate funds or assets.

These stages usually occur in sequence, but they may sometimes overlap.

There are three substantive money laundering offences in the UK:

(a) concealing, disguising, converting or transferring criminal property or removing it from the UK;

(b) entering into arrangements which a person knows or suspects will facilitate the acquisition, retention use or possession of, "criminal property" by or on behalf of another person; and

(c) acquiring, using or having possession of criminal property at an undervalue.

If any worker from the Company knows or suspects (or should have known or suspected) that another person or party is engaged in any of the activities listed directly above, then that worker is obligated to make a disclosure (see below for more details).

There is no formal definition of the term "suspects", but guidance from the courts suggests that the individual must think that there is a possibility, which is "more than fanciful", that the relevant facts exist. A vague feeling of unease would not suffice.

There is no requirement for a suspicion to be clear or firmly grounded on specific facts. If you think a transaction is suspicious, you are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. You may have noticed something unusual or unexpected and after making enquiries, the facts do not seem normal or make commercial sense. You do not have to have evidence that money laundering is taking place to have suspicion.

What might give you cause to suspect money laundering?

"Suspicious activity" is where there are circumstances that suggest that a person might be laundering money. It can include any activity that seems odd or unusual to you, or does not fit with the normal course of business. Examples of "red flags" include (but are not limited to) where:

(a) a potential contracting party is reluctant to provide supporting evidence to allow the Company to verify the legal validity of the contracting entity or the identity of key personnel;

(b) a potential contracting party presents unusual, inconsistent or suspicious due diligence documentation;

(c) a potential contracting party is not willing to disclose its ultimate beneficial owner;

(d) a contracting party or potential contracting party is reluctant to provide information in relation to the source of its funds or details of the manner in which any contribution from the Company is to be used;

(e) a potential contracting party uses numerous entities when formulating an agreement;

(f) a contracting party pays a large sum of money to the Company and requests it back for no valid, understandable reason;

(g) there is a mismatch between the contracting party's country of establishment and the location of their method of payment such as their bank account;

(h) a contracting party uses one payment method to make a payment and requests a refund to be made to a different account;

(i) a payment is made in one currency with a request that it be refunded in another currency; or

(j) a payment is conditional on particular individuals or organisations being used to do work where the Company has concerns about those individuals or organisations.

The existence of a "red flag" leading to a suspicion that money laundering is taking place does not necessarily mean that money laundering is in fact taking place. It simply means that greater scrutiny is required and that a report should be made to the Group Legal Counsel so that they can take any further steps that may be required.

Reporting Suspicions

It is important that all workers from the Company report any knowledge or suspicions they may have in relation to money laundering to the Group Legal Counsel immediately. If you form knowledge or a suspicion after a transaction has concluded, you must still report it to the Group Legal Counsel as soon as possible.

Once in receipt of a report, the Group Legal Counsel will consider it to determine whether it gives rise to grounds for knowledge or suspicion of money laundering. They will assess your report in conjunction with any other information held about the party and in light of other transaction patterns and volumes. Following this assessment, the Group Legal Counsel will make any necessary reports to the appropriate authorities.

Make no attempt to carry out an investigation yourself. Your duty is to report your knowledge or suspicion to the Group Legal Counsel and leave any necessary investigation to the law enforcement agencies.

The Group Legal Counsel will consider the matter in light of all the relevant information available within the Company and decide whether or not a disclosure needs to be made to the relevant authorities, such as the National Crime Agency (known as a "Suspicious Activity Report").

You will be advised by the Group Legal Counsel of what you are allowed to do in the circumstances.

You must never tell a person or party that you have made a report to the Group Legal Counsel; that a report has been made to the authorities; or that an investigation is in contemplation or is underway. Equally, you must not tell a person or party that there are delays whilst consent to proceed is being sought from the authorities.

If a decision is made by the Group Legal Counsel not to make a disclosure to the relevant authorities, a written record will be made, and maintained by the Group Legal Counsel, of the reason for not making the disclosure.

The Group Legal Counsel should provide an annual summary to the Board, detailing all reports made to them and any further action taken.

Terrorist Financing

Terrorist financing is the process by which terrorists fund their operations in order to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves financial support from countries, organizations or individuals. The other involves a wide variety of revenue-generating activities, some illicit, including smuggling and credit card fraud.

It is an offence to:

(a) be involved in fundraising if you have knowledge or reasonable cause to suspect that the money or other property raised may be used for terrorist purposes;

(b) use or possess money or other property for terrorist purposes, including when you have reasonable cause to suspect they may be used for these purposes;

(c) become involved in an arrangement which makes money or other property available to another if you know, or have reasonable cause to suspect it may be used for terrorist purposes; and

(d) enter into or become concerned in an arrangement facilitating the retention or control of money or other property likely to be used for the purposes of terrorism ("Terrorist Property") by, or on behalf of, another person including, but not limited to the following ways:

(i) by concealment;

(ii) by removal from the jurisdiction; and

(iii) by transfer to nominees.

It is a defence, however, if you did not know, and had no reasonable cause to suspect, that the arrangement related to Terrorist Property.

You must report your knowledge or suspicion of terrorist financing to the Group Legal Counsel as soon as reasonably practicable after the information comes to your attention. The process for reporting suspicions of terrorist financing is the same as for money laundering; see the procedure on Reporting Suspicions above. You must not disclose to donors or any third party that they are the subject of a terrorist financing report or that they are under investigation.

The Company's AML Due Diligence Procedures

The best protection against abuse by money launderers is to know who the parties to the transactions are. Anti-money laundering due diligence involves finding out who transaction parties or potential transaction parties are and understanding the source of their funds, how they are structured, who the beneficial owners are, and what their business is. The depth of the due diligence process has to be proportionate to the perceived risk – i.e. new customer vs existing customer, blue chip customers vs small local companies, activity, territory, etc.

Identification And Verification

New contracting parties must be identified prior to entering into a transaction. Corporate transacting parties are to be identified by providing their full company name, registered address, company number and website details to the Company. Individual contracting parties are to be identified by providing their name, residential address and date of birth to the Company, subject to the Global Data Protection Regulations policies and procedures.

Contracting parties' identities must be verified on the basis of documents, data or information obtained from a reliable and independent source, for example, by running credit checks by trusted third parties, by requiring a certified copy of a corporate's certificate of incorporation (or production of an individual's passport or driving licence and a recent utility bill).

The level of scrutiny must be in line with the respective risk profile – less checks (if any) would be needed for a known listed customer (working for a new to us Toyota subsidiary for example).

The Company must also take steps to establish the source of funds for higher risk transactions or unknown customers. This should be done in the first instance by asking the contracting party about the source of funds. If the explanation is reasonable and ties in with our knowledge and understanding of the contracting party or their business, no further action needs to be taken. If the explanation is unsatisfactory in any respect, proof of the source of the funds should be requested.

Due diligence should be repeated in the event that the Company develops knowledge or suspicion that the contracting party may be engaged in money laundering or terrorist financing. If due diligence cannot be completed satisfactorily, the Company must not accept funds from the contracting party. A suspicious activity report may also be required to be made to the relevant authorities.

The Company should ensure that documents, data and information that it holds are kept up to date. This means that due diligence on continuing contracting parties should be refreshed on a periodic basis (as a minimum every year) or otherwise whenever the Company becomes aware of a significant change in a contracting party's circumstances.

Ongoing Monitoring

The initial satisfactory identification of a new contracting party and knowledge of the party's source of funds is not, of itself, sufficient to protect an individual and the Company from exposure to money laundering and terrorist financing risk.

There is a continuing duty to conduct ongoing monitoring of all relationships and to be vigilant with regard to money laundering and terrorist financing at all times and to report any suspect transactions or circumstances.

Relationships with contracting parties must be subject to ongoing monitoring on a risk-sensitive and appropriate basis. This includes:

(a) scrutiny of payments made throughout the course of the relationship (including the source of funds) to ensure that they are consistent with your knowledge of the contracting party and their activities. Particular regard should be had to payments that are large and unusual or part of an unusual pattern; and

(b) updating the documents, data and other information obtained for the purpose of identifying the contracting party.

If you become aware of anything that gives rise to suspicion you must immediately invoke the Company procedures for reporting of suspicions.

Record Keeping

All documents, data and information collected to identify a contracting party and to verify their identity should be retained for at least 3 years from the date of their last involvement in a transaction, unless a local statutory requirements mandates a longer documents retention period.

Internal Controls

The Company takes its anti-money laundering and counter terrorist financing responsibilities seriously and has implemented a number of internal controls, as identified in this policy, to minimise the risk of it being used to launder the proceeds of crime or to facilitate terrorist financing. Moreover, the Company has a robust AML/CTF Training Program to educate employees in implementing and maintaining Company's AML/CTF Program. All employees undergo initial AML/CTF training when they join the Company. In addition, there are ongoing training requirements for all employees.

The Board has ultimate responsibility for monitoring these internal controls and ensuring that they are kept up to date.

The Board is also responsible for ensuring that this policy is reviewed regularly and that the procedures set out within it are up to date and in accordance with legislative and industry requirements.

Ivo Vesselinov
Group Chief Financial Officer