

GROUP ANTI MONEY LAUNDERING AND COUNTER TERRORISM FINANCING POLICY

Date: 15 February 2023

Document No. : KPHL- 23-0003

To: All employees

From: Board of Directors of Knight Piesold Holdings International Limited

Introduction

The fight against Money Laundering and Terrorism is a worldwide daily problem with which we must all engage; failure to do so brings consequences we would all prefer not to contemplate. The regulatory authorities in the UK estimate that that organised crime, each year, in the UK alone, generates approximately £90bn of illegal income.

Knight Piesold Holdings International Limited, the new Group holding company, is a company incorporated in England and it is to the laws of England that this Policy must comply but these principles are mirrored, worldwide, not only by a country's local laws but, also by series of Regulations and Directives published by the UN, the EU and the Financial Action Task Force (FATF) an international organisation which is focused on combating money laundering and terrorist financing. We MUST always comply with all such Regulations and Directives. We must also regularly monitor the list of sanctioned persons issued and maintained by these bodies.

Being engaged in capital projects with major international companies, of significant value, it might be argued that by the very nature of our business we are unlikely to become involved in activities targeted by criminals or terrorists but the process of financing terrorism and crime is not always a short term activity and for that reason, we are required to keep a watchful eye on everything we do and with everyone with whom we deal (see particularly, Politically Exposed Persons). These guidelines are not definitive, they will vary between each country within which the Group operates but these principles apply, worldwide. This is not discretionary and should be read in conjunction with the Group's anti-corruption and bribery policy.

In everything we do we must analyse the risk to our business and, of equal significance, to the impact on the Group's reputation in the event of a breach. In terms of the countries with whom we deal guidance is given by FATF which ranks and publishes a list of compliant countries: self-evidently, the lower the ranking the more vigilant we must be.

WE MUST BE ABLE TO IDENTIFY THOSE WITH WHOM WE DEAL AND CONTRACT.

Please refer any questions to your Regional Manager and to the Group Chairman in England where a central register of all client analysis and records must be maintained.

A. Key Facts

This section provides a brief overview of the main points of this Policy.

What is Money Laundering?	Money laundering is the process by which dirty money is made clean – so the true origins and ownership of money which was obtained illegally (“the proceeds of crime”) are disguised and the money then appears to come from a legitimate source.
Terrorist Financing	The most basic difference between terrorist financing and money laundering involves the origin of the funds. Terrorist financing usually uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds.
The Money Laundering Regulations (MLR)	The English MLR set out administrative requirements for the Anti-Money Laundering (AML) regime and while directly relating to the authorities including banking and legal services offer an appropriate guideline and benchmark for companies such as ours.
Proceeds of Crime Act 2002 (POCA)	The POCA came into force in February 2003. The POCA establishes a number of money laundering offences including failure to report suspected money laundering, tipping off about a money laundering investigation and prejudicing money laundering investigations.
Suspicion	You must report any suspicion you may have that money or property has originated from criminal activity regardless of whether client passes the due diligence checks. Criminal activity can be anything from terrorism and drug dealing to low level tax evasion – under declaring income etc. It is important that you do not “turn a blind eye” even if you consider what you suspect to be low level offending. Failure to report your suspicions is a criminal offence which could result in a fine, a criminal record and in the worst cases, in imprisonment. In the case of employees, at the very least you run the risk of losing your job.
General Red Flags	<ul style="list-style-type: none"> • Transactions which have no apparent purpose and which make no obvious economic sense; • In obvious terms, anything which does not fall within the usual pattern of our business must be questioned; • The wide use of offshore accounts, companies or structures in circumstances where normal business practice needs do not support such economic requirements; • Unnecessary routing of funds through third party accounts; • Unusual investment transactions without apparently discernible profit motive; • Where the client is a political figure or government official or is related to one of these;

	<ul style="list-style-type: none"> Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid the identification procedures and mask the origin of the criminal money which they wish to launder.
Consequences	<p>The Company could face significant financial penalties and in very serious cases staff could face imprisonment. A breach of the policy and hence the regulations can just as easily be caused by an administrative assistant as by a member of the management team. The safest course of action is therefore for everyone to follow the procedures set out in this Policy as a matter of routine and to raise any queries or suspicions with a Regional Manager or the Chairman.</p> <p>Failure to comply with this Policy and related procedures may lead to disciplinary action (both internal and external) and/or criminal sanctions.</p>
Risk Assessments	<p>Company’s Risk Assessment of Money Laundering and Terrorist Financing</p> <p>The Company will carry out a written risk assessment annually in order to identify and assess the risk of money laundering and terrorist financing we face.</p> <p>Matter based risk assessment</p> <p>You must undertake a Matter Based Risk Assessment for every matter on which the Company is engaged.</p>
Client Identification & Verification	<p>It is the Company’s policy to verify the identity of all new clients and all existing clients at the start of a new contract unless they have been previously identified and, you are satisfied that nothing about their situation has changed.</p> <p>The identification procedures must be carried out as soon as reasonably practicable after first contact is made with the Company. It is not necessary for the Company to wait until the verification process is complete before commencing work.</p>
Process for Client Due Diligence (CDD)	<p>Although the anti-money laundering regulations introduced in most countries contain exceptions for types of work or relationships where identity verification is not required, it is the policy of the Company to apply the identity requirements to all new clients, since the relationship may evolve into an ongoing business relationship where the evidence would be required, and it is easiest to ask for the necessary information when the relationship is first being established. Further, the universal application of the identification procedures helps the Company to avoid acting for dubious or dishonest clients for whom we would not wish to transact in any event.</p>

Enhanced Due Diligence	<p>EDD must be undertaken in the following circumstances:</p> <ul style="list-style-type: none"> • Any cases identified as high risk in the risk assessment undertaken by the Company or in relation to a project. • Any business relationship with a person established in a high-risk third country or in relation to any relevant project where either of the parties to the project is established in a high-risk third country identified by international anti-money laundering regulations (such as those introduced by the UN, EU, FATF). • Any project or business relationship with a Politically Exposed Person (PEP) or associate or family member of a PEP. • Where a client has provided false or stolen ID documents. • Where a financing of projects is/are: <ol style="list-style-type: none"> 1. Unusually complex or unusually large or follows an unusual pattern; or 2. have no apparent legal or economic purpose. • Any other case which by its nature can present a higher risk of money laundering or terrorist financing.
Understanding Purpose & Nature of the Business Relationship	<p>In relation to each project (or series of projects depending on nature of the work) the following questions should be considered:</p> <ul style="list-style-type: none"> • Is the project in question of the type that this client might be expected to do? • Is there anything unusual in client's demands (e.g. secrecy, reluctance to provide information)?
	<p>Source of Wealth</p> <p>Source of wealth relates to how the client came to have the funds in question.</p> <p>Source of Funds</p> <p>Source of funds refers to where the client's funds are received from.</p> <p>You should be satisfied the funds are consistent with the risk profile of the client without raising any suspicions to money laundering.</p>
Ongoing monitoring	<p>Ongoing monitoring is the process of keeping a client under review to ensure that the projects are consistent with your knowledge of the client, their business, and the risk profile. This means:</p> <ul style="list-style-type: none"> • Keeping the documents, data or information obtained for the purpose of applying CDD up to date.

	<ul style="list-style-type: none"> • Continuing to keep under scrutiny all the transactions undertaken during the course of the relationship and the source of funds. • Staying alert to any changes to the risk assessment undertaken at the outset of the relationship. • Staying alert to any suspicious circumstances which may suggest money laundering, terrorist financing or the provision of false CDD material. <p>It is important you keep a written record on file of any steps taken to conduct ongoing monitoring.</p>
--	---

B. Policy Aims

Top Level Commitment

You must be alert to the possibility that projects on which we are instructed may involve money laundering. It is critical that all members of staff follow the Company's Policy in order to reduce the risk of the Company facilitating or furthering such criminal activity.

Purpose of the Policy

The purpose of this Policy is to provide a set of procedures to follow to ensure that we do all we can to prevent us from doing the following:

- Handling money which is the proceeds of crime.
- Turning a blind eye to situations where we know or suspect something is not quite right.
- Tipping off a client about any knowledge or suspicion we may have.

Involvement in any of these actions, even innocent involvement, could constitute a criminal offence punishable by imprisonment. This applies to every single staff member, not just directors or senior managers.

There may also be other, less severe, consequences:

- Civil liability resulting in fines;
- Damage to reputation if our name is or appears to be, lent to such transactions;
- Claims from the true owner of property that we may have been involved in unlawful dealings;
- Claims from the UK or other authorities; and

For employees, failure to comply with this Policy and related procedures may lead to disciplinary action (both internal and external) and/or criminal sanctions.

C. Money Laundering and Terrorist Financing

Money Laundering

Money laundering is the process by which dirty money is made clean – so the true origins and ownership of money which was obtained illegally (“the proceeds of crime”) are disguised

and the money then appears to come from a legitimate source. This is generally done in three different stages:

- **Placement** — cash generated from crime is placed into the financial system i.e. paid into a bank account. This is the point at which detection is most likely. Because banks and financial institutions have developed AML procedures, criminals look for other ways of placing cash within the financial system.
- **Layering** — the structuring of complex layers of financial or commercial transactions - for example buying or selling assets such as property or shares - so as to obscure the origins of funds and to make it as difficult as possible to follow the trail created.
- **Integration** — once the origin of the funds is obscured the criminals will return them to the economy as legitimate business funds. This is the most difficult stage of money laundering to detect.

The return the criminals expect may not always be short term such that long term projects with which we are engaged may be a vehicle for laundering.

Terrorist Financing

The most basic difference between terrorist financing and money laundering involves the origin of the funds. Terrorist financing usually uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds.

D. Legal Framework

Many jurisdictions have anti-money laundering regulations of some sort. Much of the money laundering and terrorist financing legislation and regulation introduced in jurisdictions in which the Company has offices has its roots in the work of the FATF, whose standards are reflected in local legislation. In the UK these include:

i. Proceeds of Crime Act 2002 (POCA)

The POCA came into force in February 2003. The POCA establishes a number of money laundering offences including failure to report suspected money laundering, tipping off about a money laundering investigation and prejudicing money laundering investigations.

ii. The Terrorism Act 2000

The Terrorism Act establishes offences in connection with engaging or facilitating terrorism as well as raising or possessing funds for terrorist purposes. It establishes a list of organisations that the Secretary of State believes are involved in Terrorism. There is a failure to disclose offence and tipping off offences for those operating in the regulated sector for the purposes of AML/Counter-Terrorist Financing (CTF) obligations.

iii. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended by Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR)

E. The Offences

The Proceeds of Crime Act 2002 and the Terrorism Act 2000 (as amended) create a suite of principal criminal offences in relation to:

- a) the proceeds of all crimes in the UK, and

- b) property which is to be used for terrorist purposes or which is the proceeds of terrorism.

They also make it an offence not to disclose knowledge or suspicion of money laundering (except in very limited circumstances), or to "tip off" third parties about a report to the authorities, or an impending or existing investigation.

Offences also exist for conspiracy, attempt, counselling, aiding, abetting or procuring a principal offence.

Money Laundering offences

i. The primary offences

In the UK, it is an offence under the POCA to carry out any of the following "primary" money laundering activities:

- conceal, disguise, convert, or transfer criminal property, or remove it from England and Wales, Scotland or Northern Ireland;
- enter into or become concerned in an arrangement which you know, suspect or have reasonable grounds to suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person; or
- acquire, use or have possession of criminal property.

"Criminal property" is property which constitutes a person's benefit from criminal conduct, and "criminal conduct" covers all conduct which constitutes an offence in any part of the UK, or which would do so if it occurred there (although there is a defence available for certain overseas conduct if it took place in a country where it did not constitute a criminal offence at the time it occurred).

It covers not only obvious serious crimes, like the illicit sale of drugs, but also to money or savings obtained as a result of relatively minor crimes, such as regulatory breaches, minor tax evasion or benefit fraud. A deliberate attempt to obscure the ownership of illegitimate funds is not necessary.

ii. Reporting offences

The following activities are also an offence:

- where you know or suspect, or have reasonable grounds to suspect, that another person is engaged in money laundering, failure to disclose that knowledge or suspicion or reasonable grounds for suspicion as soon as possible to a Regional Manager who must report immediately, to the Chairman (the "failure to disclose" offence); or
- disclosure to a third party that a suspicious activity report has been made to the police, HM Revenue and Customs (HMRC), the National Crime Agency (NCA) or a nominated officer, or that an investigation into money laundering is being contemplated or carried out, and in both cases where the disclosure might prejudice any potential or ongoing investigation (the "tipping off" offence).

In order for there to be a failure to disclose offence, you must either know the identity of the money launderer or the whereabouts of the laundered property or believe the information on which your suspicion was based may assist in identifying the money launderer or the whereabouts of the laundered property.

Knowledge can include knowledge of circumstances which would indicate facts to an honest and reasonable person and knowledge of circumstances which would put an honest and reasonable person on enquiry.

Suspicion falls far short of proof based on firm evidence but goes beyond mere speculation. It must be based on some foundation.

Reasonable grounds to suspect is an objective test. This could include wilful blindness, or negligently failing to make adequate enquiries or failing adequately to assess the facts and information that are either presented or available and that would put an honest person on enquiry.

iii. Terrorist Financing offences

Insofar as "terrorist property" is concerned (i.e. property to be used for terrorism and the proceeds of terrorist activity), the primary offences in the UK are:

- involvement in fundraising if you have knowledge or reasonable cause to suspect that the money or other property raised may be used for terrorist purposes;
- use or possession of money or other property for terrorist purposes, including when you have reasonable cause to suspect that the property may be used for terrorist purposes;
- involvement in arrangements which makes money or other property available to another if you know or have reasonable cause to suspect that it may be used for terrorist purposes;
- entering into or becoming concerned in an arrangement facilitating the retention or control of terrorist property by, or on behalf of, another including by concealment, removal from the jurisdiction, or by transfer to nominees.

As with the POCA, it is also an offence to fail to disclose knowledge, suspicion or reasonable grounds for suspicion of a primary terrorist property offence, or to "tip off" a third party about a suspicious activity report or potential or ongoing investigation relating to terrorist property offences where the investigation might be prejudiced as a result.

F. Suspicious Activity

i. What is suspicion?

To suspect something is quite a low threshold. However, it must still have some factual foundation so is more than a "gut feeling" that something isn't quite right.

In relation to the actual money laundering offences, the test is a subjective one – it has to be proved that the person in question actually suspected that proceeds of crime were being used or that funds were destined to finance terrorist activities.

However, the offence of failing to report knowledge or suspicion is tested objectively i.e. would the facts have caused a reasonable person to suspect that another person is engaged in money laundering? This is a lower standard and therefore staff need to be on their guard.

The test is, therefore, two-fold:

- 1) Do you, as a matter of fact, have a suspicion? and

2) Would a reasonable person with your experience, background and understanding have a suspicion based on the facts as known to you?

You are not expected to police our clients - so if something comes up and client offers a reasonable explanation you do not have to corroborate that explanation (though do make a file note). But if something doesn't feel right or alarm bells are ringing do not hesitate to report to the Chairman.

ii. Reporting suspicion

You must report any suspicion you may have that money or property has originated from criminal activity regardless of whether client passes the due diligence checks. Criminal activity can be anything from terrorism and drug dealing to low level tax evasion – under declaring income etc.

It is important that you do not “turn a blind eye” even if you consider what you suspect to be low level offending. It is highly likely that it may be discovered during an internal or external audit if someone else takes over the conduct of your file or if suspicions are reported in relation to another party to a project.

Failure to report your suspicions is a criminal offence which could result in a fine, a criminal record and in the worst cases, in imprisonment. At the very least you run the risk of losing your job.

In order to protect yourself it is vital that anything you have said or done is recorded in writing. Therefore, it is important you follow all the procedures set out in this Policy and the correct procedure for reporting to the Regional Manager and the Chairman.

You will not be breaching client confidentiality or privilege by reporting any matters to the Regional Manager and the Chairman together. They will be solely responsible for determining issues relating to privilege and external reporting obligations to the NCA.

iii. Procedure for Reporting issues / suspicion to Regional Manager / Chairman

You should report any suspicious activity to the Regional Manager/Chairman where possible in writing but, where this is not immediately possible, or if the report is urgent then the report can be made initially in person, by phone or by e-mail. Please ensure if it is urgent that the message has been received by the Regional Manager/Chairman.

When completing the report, you should provide as much detail as you have relating to the circumstances that have led to your suspicions and what enquiries you have made. In the report, you should indicate whether you are wishing to proceed with the transaction and any timescale that is relevant.

The report should be emailed to both the Regional Manager and the Chairman.

Any enquiries relating to the use of these reports should be addressed to the Regional Manager and the Chairman. On receipt of the relevant report, we will consider whether to make a formal external disclosure to the NCA. You will also be providing you with guidance on the next steps to take including advice on avoiding tipping off.

Remember that once you have completed a report you must not discuss this with the client or anyone else without the written permission of the Regional Manager and the Chairman. Keep a copy of the report, but not in a public place.

iv. Communication with a client following a report

Telling your client that you have reported the matter or even discussion of any suspicion with your client is a criminal offence known as “tipping off”. It is viewed as a very serious offence and again runs the risk of imprisonment.

This also applies to any member of staff who knows that a report has been made or is being contemplated, including administrative staff.

Once you have reported the matter to the Regional Manager/Chairman you will be advised not to carry out any further work on the matter until otherwise informed. The Regional Manager/Chairman will also advise as to what to say to client should he/she make enquiries. It is important that all staff members who are aware of the report and who may be contacted by client know what they can and cannot say.

v. Communication with the police or other authorities

If you are contacted by the NCA, other law enforcement agencies, HMRC or other authorities whether by telephone or in writing, you must refer them to the MLRO immediately. It is important that you do not discuss the matter with them and that you do not provide confirmation as to whether or not the firm acts.

G. Defences

There are certain defences to the primary offences, but they are few and limited in scope. Also, there are certain exceptions/defences to the failure to disclose and tipping off offences. However, the defences are not straightforward, and you should follow the company's reporting procedures and speak to the Regional Manager/Chairman in all situations where you have a suspicion of money laundering so that he or she can make an informed decision on the appropriate course of action, and document this as necessary.

H. Consequences of non-compliance with the Money Laundering Regulations

Failure to comply with the regulations has far reaching consequences for both the Company and for its staff. The firm could face a significant financial penalty and in very serious cases staff could face imprisonment. A breach of the policy and hence the regulations can just as easily be caused by an administrative assistant as by a member of the management team. The safest course of action is therefore for everyone to follow the procedures set out in this Policy as a matter of routine and to raise any queries or suspicions with the Regional Manager/Chairman.