Anti-Money Laundering and Counter-Terrorist Financing Policy

1 Introduction

Money Laundering is the activity of disguising the origins of funds that have been gained through criminal or illicit means, so that they appear to come from a legitimate source, and can be freely used in the wider economy. It is a crime in all of the jurisdictions in which ClientEarth operates.

Terrorist Financing is a related activity, where funds of any origin may be directed towards funding a terrrorist group, and that ultimate destination of funds may be disguised as a legitimate use. It too is a crime in most jurisdictions in which we operate.

As ClientEarth grows in size, in its international scope, and in the complexity of its operations, its exposure to the risks of both money laundering and terrorist financing may increase. This policy is intended to mitigate those risks to an acceptable level.

2 Risk Context for ClientEarth

Money Laundering occurs in three stages:

- Placement - the intial stage of introducing funds into the financial system (eg, through a compromised bank account)
- Layering - the splitting and moving of funds through a complex web of transactions to disguise its origin
- Integration - the acquisition of assets through apparently "clean" funds

Terrrorism financing may follow a similar process, with the intergration stage being when they fund their terrorist activities.

As a charitable organisation with a growing international reputation, ClientEarth may be targeted by money launderers and terrorist financers because we will appear to be a legitimate source of funds, or a legitimate end point for funds. We are therefore most likely to be targeted at the Layering stage.

ClientEarth may be targeted in a number of ways, including:

1. A "donor" may donate money in one form or from one source, and then requesting a refund to another source. For example, a donor may overpay a grant donation from a bank account, and requested to be refunded to a different bank account, or by cheque. This includes legacy donations, where funds are apparently sent from the estate of a deceased person, and then we are requested to send parts of the funds back to a "relative".

2. A "donor" may attempt to control how funds are spent, through restrictions on the use of specific partners or suppliers, who in reality are the donor or their accomplacies.

3. A "donor" may wish to give us illicit funds obtained through bribery or corruption.

4. A "donor" may wish to loan us money, especially where this loan is unsolicited

5. An organisation may approach us to pass money through our account to pay another organisation

6. ClientEarth may receive an invoice from a "supplier" with bank details that we have not used before for them. This may include the details of a new supplier, but may also be the details of a current supplier that have been doctored.

7. A supplier or partner may be a terrorist or criminal organisation, but that appears to be acting legitimately.

8. In our Promoting Society or lottery operations, a player may spend a large amount of illict funds on tickets, in the expectations that a percentage will be refunded to them as prize money

3 Policy statement

ClientEarth has a zero tolerance for money laundering and terrorist financing, and will not allow itself to be a conduit for criminal or illicit funds. ClientEarth shall not support any terrorist group.

4 Risk mitigations

To mitigate these risks, ClientEarth shall:

- Maintain policies on Bribery, Fraud and other internal financial crimes to prevent it from being a source of illigetimate funds
- Maintain a Delegation of Authority, stating that any fund transfers are approved by at least two people, and that contracts are signed at an appropriate level of seniority for their value. This will help to ensure that unusual transactions are uncovered.
- Refuse the refund of any donations or grant fund amounts, other than to the original source, in the same way that funds were intially received.
- Refuse any unsolicited loans
- Refuse to allow our bank accounts to be used as a conduit for other organisation's funds
- Vet all prospective donors, suppliers, partners and employees according to our Due Dilligence Policy and Donor Acceptance Policy to ensure that the source of any major funding is legitimate, and that those who receive or handle our funds do so for legitimate reasons. This may include the checking of sanction lists where appropriate.
- Ensure the independent verification of payment details of new suppliers and partners, and any change to these details once set up.
- Ensure any external lottery manager has appropriate policies and processes in place to mitigate risks of money laundering and terrorist financing in any lotteries they operate on our behalf.
- Ensure those staff directly involved in the Promoting Society acivities of ClientEarth (including our Licence Holders) have undergone advanced anti-money laundering and counter-terrorist financing

- Maintain a Whistleblowing policy and procedure, so that any potential incidents can be uncovered. Work with our suppliers, partners and external lottery manager to ensure their own whistleblowing or suspicious activity reporting tie in with our own
- Appointed a nominated individual to be responsible for promptly and appropriately reporting money laundering or terrorist financing to the relevant authorities (including suspicious activity reporting).
- Ensuring money laundering and terrorist financing is included on our global risk register, so that it is monitored on an ongoing basis, and considered when ClientEarth introduces new processes or programmes, expands into new jurisdictions, or undergoes other material changes.
- Train all ClientEarth employees on anti-money laundering and counter terrorist financing at least once annually. This training to include their obligations to report and not to "tip-off".

5 Suspicious activity reporting

All ClientEarth employees, donors, suppliers and partners are encouraged to report any form of suspicious activity that may constiture money laundering, terrorist financing or any other crime, as soon as a suspicion arises. A suspicion does not have to be proven before it is reported.

Employees should report suspicious activity to the Director of Operations, or by following the Whistleblowing policy. We shall work with our donors, suppliers and external lottery provider to ensure they raise suspicions with us at the earliest opportunity.

ClientEarth will investigate any report of suspicious activity and report it to the relevant authorities as necessary. In the UK, this may include the police, National Crime Agency, the Charity Commission, the Gambling Commission and other regulators. Our other offices shall maintain lists of the relevant authorities for their jurisdictions. Any transaction that may constitute a suspicious activity will be suspended until the relevant authority has given permission for the transaction to continue.

ClientEarth employees, and those we work with, must take care not to "tip off" those who are conducting the suspicious activity. Tipping Off occurs when someone realises they are under investigation because of information we give them or unusual behaviour on our behalf. Tipping Off is a crime in the UK and many other jurisdictions, even if it is done unwittingly.