OCORIAN

# ANTI-FINANCIAL CRIME BRIEFING FOR DIRECTORS

OCORIAN BRIEFING

May 2017

**Directors of vehicles subject to financial regulation and/or subject to Anti-Money Laundering regulation are required to ensure compliance with a long list of requirements. This briefing seeks to set these out at a high level to assist newly appointed or those directors who have been in the same position for some time with challenging the information they receive in relation to the operation of the vehicle that they are directors of.**

Anti-Financial Crime ("AFC") encompasses a number of elements:

– Anti-Money Laundering ("AML")
– Countering the Financing of Terrorism ("CFT")
– Anti-Bribery and Corruption ("ABC")
– Anti-Tax Evasion ("ATE")

## Legislation differs

Each jurisdiction details what it considers to be criminal property or the proceeds of crime through the definitions it chooses in its legislation. It is the responsibility of a director to be aware of such definitions.

The continuing ability of a jurisdiction's finance industry to attract legitimate customers with funds and assets that are clean and untainted by criminality depends, in large part, upon the jurisdiction's reputation as being sound and well-regulated. Any business that assists in laundering the proceeds of crime whether:

– with knowledge or suspicion of the connection to crime; or
– acting without regard to what it may be facilitating through the provision of its products or services

will face the loss of its reputation, risk the loss of its licence or other regulatory sanctions (where regulated and supervised), damage the integrity of the finance industry as a whole, and may risk prosecution for criminal offences.

Each jurisdiction sets out the AFC requirements in a mix of primary, secondary and tertiary legislation and directors need to be mindful of where any one requirement sits because this can affect whether it is an obligation or guidance.

Ocorian seeks to manage such risks for itself and for vehicles to which it provides services. That said, non-Ocorian directors should seek to get comfortable that those around them understand the AFC offences and act accordingly.

## Risk Based Approach

To assist with implementing AFC regimes, regulators seek a risk based approach which:

– Recognises that the AFC threat to a regulated vehicle and its directors varies across customers, countries and territories, products and delivery channels;
– Allows differentiation between customers in a way that matches risk;
– While establishing minimum standards, allows directors to apply their own approach to systems and controls and arrangements in particular circumstances; and
– Seeks to produce a more cost effective system.

A director should consider whether the risk based approach is effectively implemented.

## Corporate Governance

Regulators require boards under the general heading of corporate governance to consider:

– Board responsibilities for the prevention and detection of financial crime;
– Requirements for systems and controls, training and awareness; and
– The appointment of a Money Laundering Reporting Officer (the "MLRO") and/ or Money Laundering Compliance Officer (the "MLCO").

To achieve the required level of systems and controls in a risk based environment the Board may demonstrate that it has considered its exposure to



CONTINUED ON FOLLOWING

financial crime risk by performing a business risk assessment:

– Involving all members of the Board in determining the risks posed by financial crime within those areas for which they have responsibility.
– Considering organisational factors that may increase the level of exposure to the risk of financial crime e.g. outsourced aspects of regulated activities or compliance functions.
– Considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation.
– Considering who its customers are and what they do.
– Considering whether any additional risks are posed by the countries and territories with which its customers are connected. Factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect financial crime will impact the risk posed by relationships connected with such countries and territories.
– Considering the characteristics of the products and services that it offers and assessing the associated vulnerabilities posed by each product and service. For example:
  • products that allow a customer to "pool" third party funds will tend to be more vulnerable - because of the anonymity provided by the co-mingling of assets or funds belonging to several third parties by the customer.
  • products such as standard current accounts are more vulnerable because they allow payments to be made to and from external parties, including cash transactions.
  • conversely, those products that do not permit external party transfers or where redemption is permitted only to an account from which the investment is funded will be less vulnerable.
– Considering the risk that is involved in placing reliance on introducers to apply identification measures.
– Considering how it establishes and delivers products and services to its customers. For example, risks are likely to be greater where relationships may be established remotely (non-face to face), or may be controlled remotely by the customer (straight-through processing of transactions).
– Considering the accumulation of risk for more complex customers.

A director should critically review such a document and also consider on an ongoing basis whether or not it is being updated to keep pace with company changes or external influences.

### Systems and Controls

Having produced a business risk assessment a board must establish and maintain appropriate and consistent systems and controls to prevent and detect financial crime, that enable it to:

– Apply CDD measures
  • identifying the customer
  • determining whether the customer is acting for a third party, whether directly or indirectly, and, if so identifying that third party
  • where the third party is a person other than an individual, understanding the ownership and control of that third party and identifying each individual who is that third party's beneficial owner or controller
  • determine appropriate identification and verification requirements
  • consider circumstances when enhanced due diligence is required and what that could consist of
  • consider the use of Simplified Due Diligence and whether its use poses an acceptable risk to the company
– Scrutinizing transactions undertaken throughout the course of a business relationship to ensure that the transactions being conducted are consistent with the relevant person's knowledge of the customer, including the customer's business and risk profile;
– Ensuring that identification documents, data or information are kept up to date;
– Report to the financial crime unit when it knows, suspects, or has reasonable grounds to know or suspect that another person is involved in financial crime, including attempted transactions;
– Adequately screening relevant employees when they are initially employed and provide training;
– Keep complete records that may be accessed on a timely basis;
– Liaise closely with the regulator and financial crime unit on matters concerning vigilance, systems and controls (including policies and procedures);
– Where applicable, communicate policies and procedures to overseas branches and subsidiaries, and monitor compliance therewith; and
– Monitor and review instances where exemptions are granted to policies and procedures, or where controls are overridden.

A director should regularly consider, based on information received, whether such controls are in place. A board may demonstrate that it checks such controls by reviewing:

– Reports presented by the MLRO/MLCO;
– Reports summarising findings from supervisory and themed examinations and action taken or being taken to address recommendations;
– The number and percentage of customers that have been assessed by the relevant person as presenting a higher risk;
– The number of applications to establish business relationships or carry-out one-off transactions declined due to CDD issues, along with reasons;
– The number of business relationships terminated due to CDD issues, along with reasons.
– Details of remediation exercises;
– Details of failures by an introducer to provide information and evidence on demand and without delay, and action taken;
– The number of alerts generated by automated on-going monitoring systems;
– The number of internal SARs made to the MLRO, the number of subsequent external SARs submitted to the financial crime unit, and timeliness of reporting (by business area if appropriate);
– Inquiries made by the financial crime unit, or production orders received, without issues having previously being identified by CDD or reporting policies and procedures, along with reasons;
– Results of testing of awareness of relevant employees with policies and procedures and legislation; and
– The number and scope of exemptions granted to policies and procedures, including at branches and subsidiaries, along with reasons.

## Culture

Directors must not only concern themselves with systems and controls but also with how the culture of a company can affect the implementation of such controls. A director may demonstrate that it has considered such cultural barriers by considering:

– Any unwillingness on the part of employees to subject high value (and therefore important) customers to effective CDD measures for commercial reasons;
– Any undue influence exerted by relatively large customers in order to circumvent CDD measures;
– Excessive pressure applied on employees to meet aggressive revenue-based targets, or where employee or management remuneration or bonus schemes are exclusively linked to revenue-based targets;
– Any excessive desire on the part of employees to provide a confidential and efficient customer service;
– The design of the customer risk classification system to ensure it does not operate in a way that avoids rating any customer as presenting a higher risk;
– Any evidence of the inability of employees to understand the commercial rationale for business relationships, resulting in a failure to identify non-commercial and therefore potential financial crime activity;
– Negative handling by managerial staff of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions;
– Any indication there is an assumption on the part of more junior employees that their concerns or suspicions are of no consequence;
– Any tendency for line managers to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily;
– Dismissal of information concerning allegations of criminal activities on the grounds that the customer has not been successfully prosecuted or lack of public information to verify the veracity of allegations;
– Whether the familiarity of employees with certain customers results in unusual or higher risk activity and transactions within such relationships not being identified as such;
– Whether there is evidence of little weight or significance attributed to the role of the MLRO/MLCO, and little cooperation between these post-holders and customer-facing employees;
– Where actual practices applied by employees do not align with policies and procedures;
– Whether employee feedback on problems encountered applying policies and procedures are ignored; and
– Non-attendance of senior employees at training sessions on the basis of mistaken belief that they cannot learn anything new or because they have too many other competing demands on their time.

Of course, for many roles, such as those directors on funds boards, the list of red flags will be much shorter.

## Outsourcing

Outsourcing poses differing risks on the ability of the company to operate its systems and controls, directors should consider these differences and document how these are managed and monitored. Each regulator publishes a document explaining what must be considered and whether notifications are required prior to such outsourcing. Directors would be wise to know these requirements prior to considering any outsourcing of functions.

## Independent Information

The board relies on the MLRO and /or the MLCO to provide independent feedback on the control environment and whether it is being suitably applied. A director should form a view on whether the MLRO has sufficient knowledge, skill, independence and resources to carry out the role. Particular emphasis should be placed on:

– Quality of board reporting
– Number and nature of internal and external reports

**Summary**

– Reviews on the systems and controls

Directors of regulated vehicles and those subject to AML oversight described above have significant responsibilities placed upon them. Out of necessity this briefing sets out the generic risks and controls which any director should be aware of. Nothing in here is exhaustive and other factors may well be in play that the director should be mindful of.

Directors are required to understand the local specifics but it is at least hoped that this briefing can act as an aide memoire for items that a director may see fit to challenge.

## KEY CONTACTS

### GLOBAL

**PAUL LEARY**
**Chief Risk Officer**
T +44 (0)1534 507200
E paul.leary@ocorian.com

**ANN SHANAHAN**
**Head of Compliance**
T +44 (0)1534 507260
E ann.shanahan@ocorian.com