Financial Services Commission
PO Box 940
Suite 3, Ground Floor
Atlantic Suites
Europort Avenue
Gibraltar
Tel (+350) 200 40283
Fax (+350) 200 40282
E-Mail: dparody@fsc.gi
www.fsc.gi
Twitter: @gibfsc

Our Ref: 031.docx/DMP

Your Ref:

22 March 2013

Dear CEO

Prevention of Financial Crime

With the bringing into effect of the Crimes Act 2011 a number of new and revised financial crimes were introduced into the statute books. This letter aims to provide regulated firms with guidance on our expectations of the systems of control that we expect to see in regulated firms in this respect.

Many of the crimes included in this letter would be a criminal offence under the Crimes Act and therefore the FSC does not purport to give guidance on the Crimes Act itself. However firms are required, under the Supervisory Acts or their secondary legislation to have adequate systems of control. The FSC considers that this extends to systems of control to prevent financial crime.

Section 6(1)(d) of the Financial Services Commission Act 2007 imposes a statutory obligation on the FSC to "*to monitor compliance by Authorised persons with legislation, rules, codes and guidance relating to the prevention of financial crime*".

The contents of this letter are non-binding and non-enforceable measures to help regulated firms mitigate the risks of their organisation being used for various types of financial crimes. These measures are appended to this letter.

The FSC has enforceable guidance in relation to Anti-Money Laundering and Combatting the Financing of Terrorism. Many of the techniques and mitigation used for these purposes are transportable in the mitigation of the other crimes which form part of this letter.

Yours faithfully,

David Parody
Deputy Chief Executive Officer

General Systems of Control

Governance

We expect senior management to take clear responsibility for managing financial crime risks, which should be treated in the same manner as other risks faced by the business. There should be evidence that senior management are actively engaged in the firm's approach to addressing the risks.

Structure

Firms' organisational structures to combat financial crime may differ. Some large firms will have a single unit that coordinates efforts and which may report to the head of risk, the head of compliance or directly to the CEO. Other firms may spread responsibilities more widely. There is no one 'right answer' but the firm's structure should promote coordination and information sharing across the business.

Risk Assessment

A thorough understanding of its financial crime risks is key if a firm is to apply proportionate systems and controls.

Policies and Procedures

A firm must have in place up-to-date policies and procedures appropriate to its business. These should be readily accessible, effective and understood by all relevant staff.

Staffing

Firms must employ staff who posses the skills, knowledge and expertise to carry out their functions effectively. They should review employees' competence and take appropriate action to ensure they remain competent for their role. Vetting and training should be appropriate to employees' roles.

Firms should manage the risk of staff being rewarded for taking unacceptable financial crime risks.

Quality of Oversight

A firm's efforts to combat financial crime should be subject to challenge. We expect senior management to ensure that policies and procedures are appropriate and followed.

Specific Systems of Control

Fraud

All firms will wish to protect themselves and their customers from fraud. Management oversight, risk assessment and fraud data will aid this, as will tailored controls on the ground. We expect a firm to consider the full implications of the breadth of fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates.

Data Security

Governance

Firms should be alert to the financial crime risks associated with holding customer data and have written data security policies and procedures which are proportionate, accurate, up to date and relevant to the day-to-day work of staff.

Controls

We expect firms to put in place systems and controls to minimise the risk that their operation and information assets might be exploited by thieves and fraudsters. Internal procedures such as IT controls and physical security measures should be designed to protect against unauthorised access to customer data.

Firms should note that we support the Information Commissioner's position that it is not appropriate for customer data to be taken off-site on laptops or other portable devices which are not encrypted.

Anti-Bribery and Corruption (ABC)

Governance

A firm's senior management is responsible for ensuring that the firm conducts its business with integrity and tackles the risk that the firm, or anyone acting on its behalf, engages in bribery and corruption. A firm's senior management should therefore be kept up-to-date with, and stay fully abreast of, bribery and corruption issues.

Risk assessment

We expect firms to identify, assess and regularly review and update their bribery and corruption risks.

Corruption risk is the risk of a firm, or anyone acting on the firm's behalf, engaging in corruption.

Policies and procedures

Firms' policies and procedures to reduce their financial crime risk must cover corruption and bribery.

Dealing with third parties

We expect firms to take adequate and risk-sensitive measures to address the risk that a third party acting on behalf of the firm may engage in corruption.

Sanctions and Asset Freezes

Governance

Senior management should be sufficiently aware of the firm's obligations regarding financial sanctions to enable them to discharge their functions effectively.

Risk assessment

A firm should consider which areas of its business are most likely to provide services or resources to individuals or entities the are subject to Sanctions.

Screening customers against sanctions lists

A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. Although screening itself is not a legal requirement, screening new customers and payments against Orders made under the Export Control Act 2005 or designated persons under the Terrorist Asset-Freezing Regulations 2011, and screening existing customers when new names are added to the list, helps to ensure that firms will not breach the sanctions regime

Matches and escalation

When a customer's name matches a person on the any of the Export Control Orders or designated persons under the Terrorist Asset-Freezing Regulations 2011, it will often be a 'false positive' (e.g. a customer has the same or similar name but is not the same person). Firms should have procedures for identifying where name matches are real and for freezing assets where this is appropriate.

Weapons proliferation

Alongside financial sanctions, the government imposes controls on certain types of trade in in Weapons of Mass Destruction. The export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is subject to strict controls under the Weapons of Mass Destruction Act 2004. Firms' systems and controls should address the proliferation risks they face.