GUERNSEY FINANCIAL SERVICES COMMISSION

8 May 2014

Presenters:

Steve Chandler – Policy Advisor, Financial Crime & Authorisations Division
Callum McVean - Senior Analyst, Financial Crime & Authorisations Division

Introduction

On 8 May 2014, the Commission and the Financial Investigation Unit ("FIU") held a co-sponsored seminar entitled "Suspicious Activity Reporting" ("SAR") which covered trends, tips, analysis and engagement. The purpose of the seminar was to provide industry, and particularly Money Laundering Reporting Officers, with the latest information in relation to SAR. The main areas which were covered included:-

- The law surrounding SAR and new, proposed changes to legislation.
- Best practice in relation to the preparation of SAR and the use of THEMIS.
- The Commission's expectations relating to firms' compliance arrangements regarding SAR.
- On-site AML/CFT visits and the Commission's role in tackling, with industry, vulnerable areas identified by SAR.

The following is a summary of the presentations made by members of the Commission. Materials relating to the presentation made by the representative from the FIU can be accessed on the Guernsey Border Agency website.

Steve Chandler
Policy Advisor, Financial Crime & Authorisations Division

My presentation today will be limited to the requirements under the Criminal Justice Proceeds of Crime Regulations and the Handbooks, as the requirements under the Disclosure and Terrorism legislation are included in the presentations made by the other speakers.

In order to comply with Regulation 15 and chapter 2 of the Handbooks, a review of compliance arrangements and their underlying policies, procedures and controls, must include those measures in place to ensure the firm and its staff's compliance with the rules in chapters 8 and 10 of the Handbooks and the reporting requirements in the Regulations.

Regulation 15 and chapter 2 of the Handbooks include certain terms which are repeated throughout. These are appropriateness and effectiveness. When reviewing their compliance arrangements, businesses are required to assess the appropriateness and effectiveness of these measures, which in this instance includes those which they have in place to comply with the requirements relating to SAR.

The Commission's expectation is that the review, as with other aspects of a firm's compliance arrangements, must comprise of an assessment of both (a) technical compliance and (b) effectiveness.

Based upon the results of the Commission's onsite visit analysis, it has been observed that the technical compliance aspect has, generally speaking, been an area where businesses are compliant. There are however, a few areas where improvements could be made.

First, procedures should be written in a manner so that they can be readily understood by the business's front line staff, not an anti-money laundering compliance specialist. In essence, businesses need to write their procedures so that they are understood by its users.

Second, the procedures should be tailored to the nature and complexity of the business.

Third, an element occasionally absent, the decision-making process related to SAR should be documented, readily accessible and most importantly, actually applied.

I will now move on to the second component of a compliance arrangements review, effectiveness. The Commission's expectation is that businesses should be able to evidence how it is that they know that their SAR procedures work. The question the Commission would ask is: What measures does the business actually take to verify that its SAR procedures work?

There are some points for businesses to consider:

1. <u>Automated systems</u>

a) Make it clear to employees that the use of an automated monitoring system does not negate the need to continue to be vigilant for possible suspicious activity. People see and hear things that make them curious and inquisitive, a system does not.
b) Be cautious about assumptions that are drawn from perceived regular patterns of activity or transactions. Just because a previously investigated event did not give rise to further concerns does not mean that a similar event in the future should not be investigated where a suspicion is formed.
c) How does the business know that there is adequate manual intervention to query changes that would not otherwise be caught by the monitoring system's programmable thresholds? Two areas to consider here are:
    - Whether the system's parameters are designed and regularly updated to alert the business to a customer's risk profile changes outside of transactions which could give rise to a suspicion, and

- Whether there is adequate manual intervention being undertaken by the staff to query risk profile changes that may otherwise not be caught by the automated monitoring system's programmable thresholds.

d) And finally are there sufficient resources to manage alerts?

2. Policies and Procedures

With regards to the effectiveness of policies, procedures and controls the positives are that, overall the Commission has observed that there is a good incorporation of rules and regulatory requirements. Most SAR policies and procedures are fit for purpose. However further improvements are required to address some of the following shortcomings identified:

a) Absence of reference to the importance of reporting attempted transactions or relationships from some SAR policies and procedures,
b) Little reference in procedures to reporting in relation to terminated business where suspicions are formed and in particular, where that closure is initiated by the customer.
c) Reviews of SAR processes is left out of the overall review of the business's compliance arrangements.
d) Outsourcing arrangements omit measures to ensure that the provider is aware of the SAR obligations in the Bailiwick.
e) Failure to have a process in place to facilitate reporting back to the MLRO by outsourcing providers where suspicions are formed arising from the services being performed.
f) Overly complex procedures with numerous checkpoint stages which end up discouraging SAR by the staff.

3. Training

The Commission onsite teams have seen an array of training material and methods on SAR. The material is frequently very concise. However, the teams have also noted on some occasions that training excludes examples of possible suspicious activity, and merely recites what is stated in the Handbook and Regulations.

In other instances, it has been noted that the training provided omits an explanation as to how customer risk reviews connect to SAR or an absence of explanation in training about the firms AML/CFT framework and where SAR fits in.

And finally, there have been a limited number of instances where training has made no mention of attempted transactions and attempts to establish business relationships, particularly where a decision has been made to reject the business.

Callum McVean
Senior Analyst, Financial Crime & Authorisations Division

My name is Callum McVean and I am a Senior Analyst in the Financial Crime & Authorisations Division's on-site team. My background before I joined the Commission was in law enforcement, working for the GBA in financial crime, as the former head of intelligence for Guernsey and I have also worked with the Home Office developing intelligence units, with protocols and procedures. I am therefore able to discuss, with knowledge, what organized criminals would be looking to achieve by targeting the Bailiwick's finance industry and the importance of having appropriate and effective controls. Due to time constraints there will not be time for many questions but there will be an e-mail address at the end for those who wish to ask any questions.

Why do criminals target the Bailiwick? Criminals do not target the Bailiwick anymore because they want anonymous accounts and the corporate veil of secrecy to hide behind us. What they now want is the British bank account, as a seal of respectability, to use as a calling card to introduce themselves into legitimate economies around the world. Organised criminals know the days of the cloak and dagger have gone. They see a well regulated industry as a challenge they are willing to rise to and to which we, the regulators, industry and law enforcement must also respond.

<u>Financial Crime & Authorisations Division</u>

The FC&A Division was formed in November 2012 with two key objectives with respect to AML/CFT – to identify weaknesses in industry that criminals/terrorists can exploit and regulate/educate industry through remediation plans and, if necessary, by enforcement action.

I am going to speak about three of the top four SAR topics and this will give you an insight into what the onsite teams are noting – with some positive messages, but also with some learning points.

<u>SAR Reporting</u>

Let's deal with a positive first. Adverse due diligence is one of the most common areas reported on. This demonstrates that customer due diligence is generally appropriate and effective: i.e. you are spotting the wolf in sheep's clothing. But this also indicates that the wolf is at the door. We noted from our review that fraud reporting has risen dramatically since 2012. This appears to be due to one factor alone, the rise in cybercrime and the technological advancement of criminals – a threat that exists at the international level. This is a common challenge for all businesses. However, onsite visit teams have in some

instances not seen a notable acknowledgement of this risk by some businesses' Boards and how it would impact their business, particularly as part of their business risk assessment.

This takes us back to what my colleague mentioned earlier regarding Regulation 15 and chapter 2 of the Handbooks and the Board's responsibility for reviewing its compliance arrangements to ensure that they are appropriate and effective.

Another large tranche of SAR is the result of reactive/defensive reporting, while another appears to be the result of new sanctions, new FATCA legislation etc. While in some instances, this appears to be a positive reaction to such changes, in other instances some reports appear to have been triggered by law enforcement enquiries and the receipt of production orders, restraints etc.

Reactive/defensive reporting is a very difficult area to fully quantify and can be viewed positively but also with concern. It can be triggered by events which are unforeseen and totally out of the control of the Board – sanctions, new FATCA agreements etc. However, they are also on occasion the result of law enforcement enquiries that can, but not always, highlight issues that should have been picked up during customer risk reviews.

Onsite Visits - Customer Risk Reviews

Let us look first at what the Regulations say about customer risk reviews - Regulation 3(2)(b) states that a financial services business must regularly review any risk assessment carried out under subparagraph (a) (*prior to the establishment of a business relationship)* so as to keep it up to date and, where changes to that risk assessment are required**, it must make those changes.**

Onsite teams have noted that customer risk reviews, in some instances, are not being conducted with sufficient scrutiny and analysis to detail what the **actual** risks are to the business and how the business will use this analysis of the risks to implement effective, specific risk mitigation controls. It appears that, in some instances, once the good work has been done at the outset of a business relationship, subsequent reviews rate low in a Board's priority and more focus is placed on gaining new business.

It seems counter-productive to go to the effort of having a formal review and not complete this review thoroughly – the Commission is not asking industry to be risk averse, rather we want industry to be risk alert. Reviews should not be seen as a tick box exercise, where the Handbook is used simply as an inventory to follow. It is the interpretation of the facts required under the Handbook which is the key to this message and the determination following a review of "what are the risks of doing business with this customer?".

It is of critical importance that businesses address changes to a customer's risk profile during the ongoing life cycle of a client/customer. Failure to do so leaves businesses vulnerable to criminal/terrorist exploitation, which can affect the business, its controllers and the Bailiwick as a finance centre.

Thank you.