Chapter 4

Automated Anti-Money Laundering Transaction Monitoring Systems (2007)

4.3 Consolidated examples of good and poor practice

4.3.1 This report contained the following Examples of good practice:

4.3.2 Statement of good practice

•Depending on the nature and scale of a firm's business activities, automated AML TM systems may be an important component of an effective overall AML control environment.

Methodologies

•TM systems use profiling and/or rules-based monitoring methods.

•Profiling identifies unusual patterns of customer activity by applying statistical modelling techniques. These compare current patterns of activity to historical activity for that customer or peer group.

•Rules-based monitoring compares customer activity to fixed pre-set thresholds or patterns to determine if it is unusual.

Development and implementation

•A clear understanding of what the system will deliver and what constraints will be imposed by the limitations of the available data (including any issues arising from data cleanliness or legacy systems).

•Consideration of whether the vendor has the skills, resources and ability to deliver the promised service and provide adequate ongoing support.

•Maintenance of good working relations with the vendor, e.g. when collaborating to agree detailed system configuration.

•Use of recommended hardware, not necessarily a firm's own standard, to reduce processing problems, or otherwise finding a solution that is a good fit with a firm's existing infrastructure.

•A full understanding of the data being entered into the system and of the business's requirements.

•Regular housekeeping and database maintenance (operational resilience is vital to ensure that queries do not back up).

•Careful consideration of the risks of commissioning a bespoke vendor system, which may be incompatible with future standard product upgrades.

•Continued allocation of sufficient resources to ensure manual internal suspicion reporting is effective, as TM can supplement, but not replace, human awareness in day-to-day business.

Effectiveness

•Analyse system performance at a sufficiently detailed level, for example on a rule-by-rule basis, to understand the real underlying drivers of the performance results.

•Set systems so they do not generate fewer alerts simply to improve performance statistics. There is a risk of 'artificially' increasing the proportion of alerts that are ultimately reported as suspicious activity reports without generating an improvement in the quality and quantity of the alerts being generated.

•Deploy analytical tools to identify suspicious activity that is currently not being flagged by existing rules or profile-based monitoring.

•Allocate adequate resources to analysing and assessing system performance, in particular to define how success is measured and produce robust objective data to analyse performance against these measures.

•Consistently monitor from one period to another, rather than on an intermittent basis, to ensure that performance data is not distorted by, for example, ad hoc decisions to run particular rules at different times.

•Measure performance as far as possible against like-for-like comparators, e.g. peers operating in similar markets and using similar profiling and rules.

Oversight

•Senior management should be in a position to monitor the performance of TM systems, particularly at firms that are experiencing operational or performance issues with their systems, so that issues are resolved in a timely fashion.

•Close involvement of the project management process by major business unit stakeholders and IT departments is an important component of successful system implementation.

Reporting & review

•There should be a clear allocation of responsibilities for reviewing, investigating and reporting details of alerts generated by TM systems. Those responsible for this work should have appropriate levels of skill and be subject to effective operational control and quality assurance processes.