HONG KONG MONETARY AUTHORITY
香港金融管理局

# Q & As raised during the AML Forum 2017 on 6th July 2017

*[Remarks: This is the text of the Q & A session as drafted and may differ slightly from the delivered version]*

1) **What is the status of the Guidance and how should it be used?**

   The Guidance is intended to be used as a starting point for AIs in their approach to the issue of Trade-based Money Laundering (TBML). The Guidance is not intended to be used as a definitive checklist but as a reference guide, an approach which recognises each AI is unique in terms of the specific risks they face, based on factors such as, but not limited to customer segments, product offerings, etc. AIs should take a risk-based approach when implementing policies and procedures tailored for their operations and this guidance forms part of such an approach.

2) **Are AIs required to subscribe to a screening system to screen dual use goods in order to meet the HKMA requirements / expectations?**

   No strict requirement exists; the procedures and processes deployed will vary from AI to AI depending on a variety of factors. The expectation is that AIs should develop situational awareness, through assessment of the risks they are exposed to and put in place adequate systems and controls to mitigate those risks (and such a screening tool may or may not form part of those controls). AIs need to evaluate their own situation and decide what role an automated system could play, if any, and whether this would increase effectiveness.

3) **How far do you expect your payments screening / trade processing staff to investigate into different TBML / Sanctions issues?**

   HKMA has reiterated that it does not expect a ‘zero failure’ outcome in any anti-money laundering (AML) work conducted by AIs, and this principle applies equally in the area of trade controls. The messages in the HKMA’s circular of 8 September 2016 on De-risking and Financial Inclusion are applicable, that AML work should be based on the principles of risk differentiation, proportionality and reasonableness.

There is no requirement that AIs will prove all trade transactions as genuine in order to identify the few which may not be; this is not how any effectively functioning AML system is supposed to work. The expectation is to understand what may be higher risk and/or suspicious and have appropriate processes in place by way of response. AIs are not required to reject business and / or exit customers at the slightest sign of irregularity, although more may need to be done in such cases; cases in which a customer or transaction are rejected purely because of ML concerns should be the exception.

4) **How can AIs determine the market price of the goods traded, and how can the risk of under / over-invoicing be mitigated?**

The guidance is clear that such actions are risk-based, and that determining the market price of goods is not a fixed requirement. AIs should consider first if they have any internal guidance relating to this matter. Effective CDD is also useful; collecting information from customers to know the types of goods they expect to trade in, prices that they are trading at, etc. could also help AIs understand normal behavioural patterns of their customers.

5) **Are there any specific things to look at when conducting CDD in the context of TBML?**

Since the AI's ability would depend on the nature of relationship, this comes back to the principle of KYC, where AIs would need to understand counterparties, such as suppliers and buyers etc. Additionally, looking at negative news is one way that could assist efforts in combatting TBML; however, this should be done using a risk based approach and AIs should not take this away as a mandatory requirement.

6) **How do you train staff to recognize potential TBML signs?**

The issue of TBML needs to be viewed as a part of wider AML/CFT compliance; consequently, the experience of staff in performing trade finance-related work is important but over reliance should not be made on this aspect alone.

Stakeholders to trade finance usually are in both Trade and Compliance departments. The former is familiar with trade products but may be less well-versed in AML/CFT requirements, and vice versa. This frequently leads to misunderstanding between the two parties, and AIs could consider:

- Holding sessions to bring these two groups of people together, share best practice and understanding, and work out issues between and common to them
- Providing targeted training to each group, to get both sides to understand each other's concerns.

It is also important to note that training people to simply recognize "red flags" may not be the best approach and can sometimes produce the wrong outcome. Communication, sharing and training staff to understand the broader picture is key, which should involve indicators of both higher and lower risk activity.

During the forum one AI talked about a suggested practice in that a cue card had been developed for staff on which some key considerations were detailed that could be referenced when reviewing documents. The key point made was the purpose of the card; it was not meant to be a checklist, but to prompt the staff member to consider certain issues and to raise their levels of awareness and consistency in applying certain process. But training had been provided to ensure the 'cues' were not applied mechanically.

**7) What can AIs do to improve the situation?**

AIs can consider the following factors when looking at ways to improve their situation. The following points are non-exhaustive:

- Ensuring adequate risk assessment and understanding of their customers
- Ensuring an effective AML system, particularly in identifying high-risk customers, in accordance with a risk based approach, and ensuring effective and proper use of CDD information.
- Establishing clear policies and procedures to deal with TBML risks
- Developing targeted trade finance financial crime training for relevant staff
- Establishing QA processes over TBML related decision-making processes.

## Useful References:

“Typologies Report on Proliferation Financing” Financial Action Task Force. 2008. http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

Dall et al. “Countering Proliferation Finance: An Introductory Guide for Financial Institutions” Royal United Services Institute. 2017. https://rusi.org/sites/default/files/201704_rusi_cpf_guidance_paper.1_0.pdf

Dall et al. “Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance” Royal United Services Institute. 2016. https://rusi.org/sites/default/files/201606_whr_3_16_countering_proliferation_finance_v2_0.pdf

United Nations Security Council – Report of the Security Council Committee established pursuant to resolution 1540 (2004) (December 2016) http://daccess-ods.un.org/access.nsf/GetFile?OpenAgent&DS=S/2016/1038&Lang=E&Type=DOC

United Nations Security Council – Report of the Panel of Experts established pursuant to resolution 1874 (2009) (February 2017) http://daccess-ods.un.org/access.nsf/GetFile?OpenAgent&DS=S/2017/150&Lang=E&Type=DOC