

Cover Payment Messages related to Cross-border Wire Transfers

1. Introduction

- 1.1 The processing of cross-border wire transfers usually involves several financial institutions. In addition to the originator's bank and the beneficiary's bank, additional financial institutions (cover intermediary banks) which provide correspondent banking services to the originator's bank or the beneficiary's bank are often involved in the settlement of cross-border wire transfers. Cover payment messages are messages used by these financial institutions for the purpose of arranging funding to settle the interbank payment obligations created by cross-border wire transfers.
- 1.2 This paper sets out the Hong Kong Monetary Authority (HKMA)'s supervisory expectation in relation to the processing of cross-border wire transfers by authorized institutions (AIs), focusing on the responsibilities of their respective roles in handling cover payment messages:
 - (i) AIs acting on behalf of the originator (ordering AIs);
 - (ii) AIs providing correspondent banking services to either the originator's bank or the beneficiary's bank (cover intermediary AIs); and
 - (iii) AIs acting on behalf of the beneficiary (beneficiary AIs).

The paper is based on the Basel Committee on Banking Supervision's paper on "Due diligence and transparency regarding cover payment messages related to cross-border wire transfers" issued in May 2009.

- 1.3 In processing cross-border wire transfers, AIs should comply with the requirements specified in this paper, in addition to the relevant provisions contained in the Guideline on the Prevention of Money Laundering (Guideline) and the Supplement to the Guideline on the Prevention of Money Laundering (Supplement) issued by the HKMA.
- 1.4 This paper will be effective from **8 February 2011**.

2. Responsibility of ordering AIs

- 2.1 Ordering AIs should ensure that cross-border wire transfer messages contain the originator information specified in paragraph 9.2 of the Supplement, save in the circumstances described in paragraph 9.3 of the Supplement.
- 2.2 Ordering AIs should undertake customer due diligence on the originator in accordance with the requirements of the Guideline and the Supplement.
- 2.3 Ordering AIs should ensure that the messages they send to cover intermediary banks contain originator and beneficiary information. The originator and beneficiary information included in the cover payment message should be identical to that contained in the corresponding direct cross-border wire transfer message sent to the beneficiary's bank. Ordering AIs are encouraged, where

possible, to include other identity information about the beneficiary in cover payment messages, where this is necessary to limit the risk of customer assets being incorrectly frozen, blocked or rejected, or of the cover payment being unduly delayed.

2.4 Ordering AIs should establish clear policies on the processing of cross-border wire transfers. The policies should address the following issues:

- (i) record keeping;
- (ii) the verification of originator's identity information¹;
- (iii) the message formats and the circumstances in which the formats should be used; and
- (iv) the information to be included in messages.

2.5 Ordering AIs should include cross-border wire transfers in their ongoing due diligence on the business relationship with the originator and in their scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with their knowledge of the customer, its business and risk profile. Ordering AIs may adopt a risk-based approach in their ongoing due diligence process. The process should be subject to regular audits to ensure its effectiveness.

Responsibility of cover intermediary AIs

3.1 With effect from 21 November 2009, completion of the originator and beneficiary fields in SWIFT's MT202 COV is mandatory. If these fields are left blank the cover payment message will automatically be rejected by SWIFT.

3.2 Where other systems are used, cover intermediary AIs should establish clear policies and procedures to ensure, in real time, that the relevant fields for storing originator and beneficiary information in cross-border cover payment messages are not blank.

3.3 Where such fields are blank, cover intermediary AIs should consider taking one or more of the following actions:-

- (i) declining to process the transaction;
- (ii) obtaining the missing information from the originator's bank or the preceding cover intermediary bank as the case may be;
- (iii) filing a suspicious transaction report with the Joint Financial Intelligence Unit (JFIU).

¹ Where an originator is a non-account holder, AIs should follow the customer identification, verification and record keeping requirements prescribed for wire transfers in the Guideline on Prevention of Money Laundering and its Supplement.

The decisions taken and the reasons for them should be properly documented.

- 3.4 Cover intermediary AIs should screen the originator and beneficiary names against their database of terrorists and terrorist suspects, which should include the individuals and entities designated under the United Nations (Anti-Terrorism Measures) Ordinance or the Regulations made under the United Nations Sanctions Ordinance.
- 3.5 A cover intermediary AI may rely on its correspondent bank to screen the originator and beneficiary names, provided that it is satisfied with the effectiveness of the correspondent bank's screening procedures and related controls. The cover intermediary AI should bear in mind at all times that it remains primarily responsible for compliance with anti-money laundering and counter terrorist financing legislation in Hong Kong even though it has outsourced the screening function to another party. The cover intermediary AI should consult the HKMA in advance on any outsourcing proposal and ensure compliance with the requirements set out in the Supervisory Policy Manual (SA-2) on Outsourcing. In particular, the respective responsibilities of the cover intermediary AI and its correspondent bank should be set out clearly in writing. The cover intermediary AI should undertake regular reviews to ensure that it remains satisfied as to the effectiveness of its correspondent bank's screening procedures and related controls. This may be done, for example, by conducting its own screening on the originator and beneficiary names on a sample and ex post basis.
- 3.6 Cover intermediary AIs should develop and implement policies and procedures to monitor if the originator and beneficiary information included in cross-border cover payment messages is manifestly meaningless or incomplete. The monitoring may be done on a risk sensitive basis, subsequent to the processing of the transactions.
- 3.7 Where cover payment messages are found to contain manifestly meaningless or incomplete originator or beneficiary information, cover intermediary AIs should consider taking one or more of the following actions:
 - (i) Contacting the originator's bank or preceding cover intermediary bank as the case may be to clarify and obtain the necessary information about the originator and the beneficiary;
 - (ii) Considering, in the case of repeated incidents involving the same institution or in cases where the originator's bank or preceding cover intermediary bank refuses to provide the required information, whether or not the correspondent relationship with the institution should be restricted or terminated;
 - (iii) Filing a suspicious transaction report with the JFIU.

The decisions taken and the reasons for them should be properly documented.

- 3.8 Cover intermediary AIs should monitor, on a post-transaction and risk-based

approach, the transactions which they process to identify patterns of activity that may be suspicious, and report them to the JFIU where appropriate. Where such transactions are associated with a particular correspondent, the relationship with the correspondent should be reviewed.

4. Responsibility of beneficiary AIs

- 4.1 Beneficiary AIs should identify the beneficiary and verify its identity in accordance with the requirements in the HKMA's Guideline and Supplement.
- 4.2 Beneficiary AIs should have effective risk-based procedures in place to identify wire transfer lacking complete originator information. They should take into account the lack of sufficient originator and beneficiary information or other transparency problems in assessing whether a wire transfer or related transactions are suspicious, and report them to the JFIU where appropriate. Beneficiary AIs should consider restricting or even terminating their relationships with financial institutions that fail to meet international transparency standards relating to cross-border wire transfers.

Hong Kong Monetary Authority
February 2010