HSBC Bank Australia Limited

Statement on Anti-Money Laundering and Counter-Terrorism Financing

HSBC Bank Australia Limited (HSBC) is required by law to comply with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* ("AML/CTF Act"), and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* ("AML/CTF Rules").

The AML/CTF legislation is regulated by the Australian Transactions Reports and Analysis Centre ("AUSTRAC") and has been introduced to align Australia with international standards on the prevention, detection and reporting of money laundering and terrorism financing.

HSBC is also required to comply with the *International Trade and Integrity Act 2007.* HSBC may be required, from time to time, to comply with the relevant provisions of the *Hong Kong Monetary Authority Guideline on the Prevention of Money Laundering* (as amended) and the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act 2001*.

HSBC's AML/CTF compliance programme to meet the above requirements, which is overseen by a specially designated AML/CTF compliance officer, is underpinned by the Group's Global Policy and Principles, detailed below.

HSBC Global Policy and Principles

The HSBC Group's (the Group) global policy is to comply with high standards of anti-money laundering (AML) practice in all markets and jurisdictions in which it operates, and to comply with both the specific provisions and the spirit of all relevant laws and regulations.

This policy applies not only to money laundering related to the proceeds of crime, but also to terrorist financing, and all references to money laundering and AML in the HSBC Group Money Laundering Deterrence Global Policy and Principles (GPPs) include terrorist financing.

The policy reflects the Financial Action Task Force on Money Laundering (FATF) 40 Recommendations to combat money laundering and the 9 Special Recommendations to counter terrorist financing.

The GPPs set minimum standards and apply to all staff and businesses of the Group. In any jurisdiction where local money laundering requirements are set at a lower standard than the Group's, then the Group's standards shall apply in addition to those local standards.

The following are the main elements of the policy:

Customer Due Diligence

Before doing business with any prospective customer, appropriate customer due diligence (CDD) is required to be undertaken and recorded. The CDD process comprises (a) the identification and appropriate verification of identity of the customer (and, where different, beneficial owner) and any other relevant parties and (b) additional and appropriate Know Your Customer (KYC) information, applying a risk-based approach.

(a) A prospective customer's identity should be obtained and verified using reliable, independent documentary and/or electronic source material. Without such, the business should be declined. Customer identification procedures for non-face to face business should include appropriate measures to mitigate the risks posed by such business. Members of the Group screen customers against lists of terrorist and sanctioned names issued by major Competent Authorities.

(b) Appropriate KYC information is required to be obtained prior to commencing the relationship and, applying a risk-based approach, updated on a regular basis during the course of the business relationship. KYC information includes, but is not limited to, appropriate personal, business, and financial details with regard to the customer, details on the purpose and intended nature of the business relationship, including anticipated

transactional activity, details as to the source of funds/wealth. Members of the Group are required to subject customers regarded as high risk for any reason to enhanced CDD.

HSBC Bank Australia Limited

Statement on Anti-Money Laundering and Counter-Terrorism Financing

In no circumstances may accounts be operated or relationships established for anonymous customers or in obviously fictitious names or for a shell bank as defined by the FATF.

Identification of Suspicious Transactions

It is a requirement that appropriate scrutiny and monitoring of transactions, account activity and customers are undertaken in order to identify unusual and potentially suspicious activity.

Monitoring of transactions and account activity are undertaken applying a risk-based approach and having regard to the size and nature of the Group's member's business.

Transactions and account activity involving customers regarded as high risk are the subject of enhanced monitoring.

Reporting of Suspicious Transactions

Every business unit in the Group is required to have procedures in place so that any transactions and/or activities which are believed to be suspicious are reported to a central Money Laundering Reporting Office function where the suspicions will be validated. If there are local legal or regulatory requirements for reporting suspicious transactions/activities, all validated cases are to be reported as required.

Maintaining Records

Adequate records are required to be maintained to demonstrate that appropriate and ongoing CDD procedures have been followed, and to reconstruct transactions. These records are required to be maintained for at least 5 years after the relationship has ended or after the date of the transaction, or such longer period as required by local law or regulation.

Payment Screening

In order to comply with sanctions and with lists of known or suspected terrorists issued by the UN and by Competent Authorities, the Group's businesses are required to ensure that payments are subject to real time pre-execution screening against the Group minimum requirement list, and against any other sanctions/lists issued by local Competent Authorities. Appropriate action is required to be taken when a positive match has been established.

Specific businesses and customers

The Group has established a number of minimum standards in relation to AML controls for certain types of businesses and customers, e.g. Correspondent Banking, Private Banking etc. which are applicable to all relevant members of the Group.

Training

Members of the Group are required to provide all new staff including temporary or contract staff who may be involved in customer business with suitable and timely induction training and refresher training to ensure that they understand the Group's approach to money laundering deterrence.

Staff in high-risk areas are required to receive appropriate training to enable them to understand the money laundering techniques which are likely to be used in their area, and to remind them of their personal responsibilities.

Monitoring and Review of Money Laundering Deterrence

Regular monitoring is required to be undertaken by line management and/or Compliance to check that all businesses are complying with the GPPs and with local legal and regulatory requirements. Operational and functional review work will be undertaken by Compliance and/or Audit functions, as appropriate. The level and frequency of monitoring and review work is required to be determined having regard to materiality and risk in relation to the business and customer base.