FINANCIAL SUPERVISORY COMMISSION

Cook Islands

PRUDENTIAL STATEMENT

No. 08-2006

CUSTOMER DUE DILIGENCE

1. Consistent with ensuring that banks operating in the Cook Islands implement sound risk management practices, the Financial Supervisory Commission requires all domestic and international banks to incorporate the principles and recommendations outlined in this Guideline into their risk management policies. The objective of this guideline is to ensure that banks have in place know-your-customer (KYC) policies. This guideline is based on principles outlined by the Basel Committee on Banking Supervision in its paper, "*Customer due diligence for banks*" issued in October 2001.

2. In addition to the requirements of this guideline, banks are also expected to comply with the requirements of the Banking Act (2003) and the Financial Transactions Reporting Act (2004).

BACKGROUND

3. Internationally, supervisors are increasingly recognising the importance of ensuring that banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

4. KYC is most closely associated with the fight against money-laundering. The Commission's approach to KYC is from a wider prudential, not just anti-money laundering or financing of terrorism, perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for unusual activities which may result in suspicious transaction reports.

ESSENTIAL ELEMENTS OF KYC STANDARDS

5. All banks are required to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements. Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

Customer acceptance policy

6. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers.

Customer identification

7. Customer identification is an essential element of KYC standards. For the purposes of this guideline, a customer includes:

    - The person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);
    - The beneficiaries of transactions conducted by professional intermediaries; and
    - Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

8. Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified.

9. Banks should document and enforce policies for identification of customers and those acting on their behalf. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present for interview. A bank should always ask itself why the customer has chosen to open an account in the Cook Islands.

10. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, banks should undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

11. Banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers, supervisors and auditors.

12. Banks should develop clear standards on what records must be kept on customer identification and individual transactions and their retention period. Such a practice is essential to permit a bank to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution. Banks should obtain customer identification papers and retain copies of them for at least six years after the account is closed or the business relationship ceases. As required under Section 6 of the Financial Transactions Reporting Act, banks must keep records of every transaction that is conducted through it and must retain records for a minimum period of six years from the date of any transaction or correspondence. Section 6 of the Financial Transactions Reporting Act also specifies the type of transaction data that must be retained by banks.

13. Banks should subject transactions with customers in jurisdictions that do not have adequate systems in place to prevent or deter money laundering or financing of terrorism to additional scrutiny to examine the background and purpose of the transaction.

GENERAL IDENTIFICATION REQUIREMENTS

14. Banks should obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.

15. When an account has been opened, but problems of verification arise in the banking relationship that cannot be resolved, the bank should close the account and return the monies to the source from which they were received. Pursuant to section 4 of the Financial Transactions Report Act the bank has an obligation to identify and verify the customer when

entering a continuing business relationship, or in the absence of such a relationship, when the customer conducts any transaction. Where the identification and verification process is not completed the bank is obliged, pursuant to section 5 of the Financial Transactions Reporting Act, to report the matter to the Financial Intelligence Unit.

16. Banks should include originator information and related messages on funds transfers which will remain with the transfer throughout the payment chain. Originator information should include name, address, and account number (when being transferred from an account). Banks should give enhanced scrutiny to inward funds transfers that do not contain originator information. Should problems of verification arise that cannot be resolved, the bank should return the monies to the source from which they were received. Where identification and verification are not completed the bank is obliged to report the matter to the Financial Intelligence Unit.

17. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced diligence procedures to the customer.

18. Banks must not open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. In accordance with the Financial Transactions Reporting Act section 7, all accounts must be maintained in the true name of the account holder. Confidential numbered accounts are not acceptable.

SPECIFIC IDENTIFICATION ISSUES

19. There are a number of more detailed issues relating to customer identification, which are outlined below. The Commission will monitor international developments and issue further guidelines and/or guidance notes on the matter.

Personal customers

20. In developing customer identification requirements, banks need to consider the client's circumstances and it may be appropriate to impose higher standards on non-resident or expatriate customers than would be applied to Cook Islands residents. As noted in paragraph 14, banks need to ensure that customer identification requirements are sufficient to allow them to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. For personal customers, banks should at a minimum seek to obtain from clients the following information to verify the client's identification:

- Name and/or names used,
- Permanent residential address,
- Date and place of birth,

- Name of employer or nature of self-employment/business,
- Specimen signature
- Evidence of current physical address such as copies of utility (electricity, phone etc) accounts, and
- Source of funds.

21. Additional information would relate to nationality or country of origin, public or high profile position, etc. Banks should verify the information against original documents of identity issued by an official authority (examples including identity cards, passports and photo driver's licence). Such documents should be those that are most difficult to obtain illicitly. Where there is face-to-face contact, the appearance should be verified against an official document bearing a photograph. Any subsequent changes to the above information should also be recorded and verified. Copies of photographic evidence of identity must be clear and be "useable" for identification purposes.

Corporate and other business customers

22. For corporate and other business customers, banks should obtain evidence of their legal status, such as an incorporation document, partnership agreement, association documents or a business licence. For large corporate accounts, a financial statement of the business or a description of the customer's principal line of business should also be obtained. In addition, if significant changes to the company structure or ownership occur subsequently, further checks should be made. In all cases, banks need to verify that the corporation or business entity exists and engages in its stated business. The original documents or certified copies of certificates should be produced for verification.

Trust, nominee and fiduciary accounts

23. Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood. Banks should establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include the trustees, settlors/grantors and beneficiaries.

Corporate vehicles

24. Banks should be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international companies, may make proper identification of customers or beneficial owners difficult. A bank should understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

25. Banks should exercise care in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all such companies should be obtained. In the case of entities that have a significant proportion of capital in the form of bearer shares, extra vigilance is required. A bank may be completely unaware that the bearer shares have changed hands. Therefore, banks should put in place satisfactory procedures to monitor identity of material beneficial owners. This may require the bank to immobilise the shares, e.g. by holding the bearer shares in custody.

Introduced business

26. The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some instances, banks may rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. Banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

27. Banks that use introducers should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out in this guideline. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:

- It must comply with the minimum customer due diligence practices identified in this guideline;
- The customer due diligence procedures of the introducer should be as rigorous as those which the bank would have conducted itself for the customer;
- As required by the Financial Transactions Reporting Act section 4(7)(c), the introducer must be regulated and supervised, and have measures in place to comply with the requirements of sections 4, 5 and 6 of the same Act.
- The bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- The bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- All relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the bank, which must carefully review the documentation provided. Such information must be available for

review by the supervisor and the Financial Intelligence Unit, where appropriate. In addition, banks should conduct periodic reviews to ensure that an introducer that it relies on continues to conform to the criteria set out above.

Client accounts opened by professional intermediaries

28. When a bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

29. Banks often hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Banks also hold pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the bank, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

30. Where the funds are co-mingled, the bank should look through to the beneficial owners. There can be circumstances where the bank may not need to look beyond the intermediary, for example, when the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base, as the bank. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, the bank should apply the criteria set out in paragraph 27 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

31. Where the intermediary is not empowered to furnish the required information on beneficiaries to the bank, for example, lawyers bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this guideline or to the requirements of the Financial Transactions Reporting Act or anti-money laundering legislation in other jurisdictions, then the bank should not permit the intermediary to open an account.

Politically exposed persons

32. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.

33. Accepting and managing funds from corrupt PEPs will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of the Cook Islands' financial system. In addition, a bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual

assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, a bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

34. Banks should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level.

Non-face-to-face customers

35. Banks are on occasion asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

36. A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, the Financial Supervisory Commission expects that banks proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.

37. In accepting business from non-face-to-face customers:

- Banks should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview; and
- There must be specific and adequate measures to mitigate the higher risk.

Examples of measures to mitigate risk include:

- Certification of documents presented;
- Requisition of additional documents to complement those which are required for face-to-face customers;
- Independent contact with the customer by the bank;
- Third party introduction, e.g. by an introducer subject to the criteria established in paragraph 27; or
- Seeking verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds.

ON-GOING MONITORING OF ACCOUNTS AND TRANSACTIONS

38. On-going monitoring is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, banks are likely to fail in their duty to report suspicious transactions where they are required to do so under the Financial Transactions Reporting Act. The extent of the monitoring needs to be risk-sensitive. For all accounts, banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account.

39. There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

- Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. For example, the types of reports could include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.

- Senior management in charge of private banking business should know the personal circumstances of the bank's high-risk customers and be alert to sources of third party information. A senior manager should approve significant transactions by these customers.

- Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

RISK MANAGEMENT

40. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of

the bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures are managed effectively. Banks are obliged to appoint a Money Laundering Reporting Officer to ensure compliance with the requirements of the Financial Transactions Reporting Act. The Banks' obligations include internal training, establishment and maintenance of procedures and systems to implement Sections 4, 6-8, 10, and 11 of the Financial Transactions Reporting Act, screening of prospective employees, and audit function to test AML/CFT systems and procedures.

41. Banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. The Financial Supervisory Commission expects that a bank's compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management, the Board of Directors or, in the case of foreign bank branches appropriate officers outside the Cook Islands, if it believes management is failing to address KYC procedures in a responsible manner.

42. Internal audit plays an important role in independently evaluating the risk management and controls, through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training.

43. Banks are required to have an ongoing employee-training programme so that bank employees are adequately trained in KYC procedures. Banks should put in place measures to ensure that employees are aware of domestic laws and regulations relating to money laundering and the financing of terrorism. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments.

44. External auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice. Under the Banking Act banks' external auditors have obligations to report to the Commission whether all prudential standards have been observed, including the requirements of this Guideline.

THE ROLE OF FINANCIAL SUPERVISORY COMMISSION

45. The Financial Supervisory Commission has a responsibility to monitor whether banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Under its powers to conduct on-site examinations, provided under Section 15 of the Banking Act, the Financial Supervisory Commission will be seeking to satisfy itself that appropriate internal controls are in place and that banks are in compliance with supervisory and regulatory guidance. The review process will include not only a review of policies and procedures but also a review of customer files and the sampling of some accounts.

IMPLEMENTATION OF KYC STANDARDS IN A CROSS-BORDER CONTEXT

46. The Financial Supervisory Commission expects banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors.

47. However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, internal auditors and compliance officers from both local and head offices as appropriate should support him.

This Prudential Statement is issued effective 20 March 2006.

FINANCIAL SUPERVISORY COMMISSION
20 March 2006

Revised 9 May 2006