MONEY LAUNDERING PREVENTION REGULATIONS 2009

SAMOA

Arrangement of Provision

PART I
PRELIMINARY

1. Title and Commencement
2. Interpretation
3. Application
4. Verification of customer identity

PART II
CUSTOMER DUE DILIGENCE

5. Customers who are natural persons
6. Customers who are legal persons
7. Insurance
8. Non face to face customers
9. Determination of person on whose behalf the customer is acting
10. Delay in verification of customers
11. Reliance on third parties or intermediaries
12. On going due diligence
13. Ongoing monitoring of customers
14. Enhanced customer due diligence for higher risk customers, business relationships and transactions
15. Simplified customer due diligence for lower risk customers

PART III
REPORTING OF TRANSACTIONS AND INFORMATION

16. Originator information requirements

PART IV
INTERNAL PROCEDURES, POLICIES, SYSTEMS AND CONTROLS

17. Adoption and implementation of internal procedures, policies, systems and controls
18. Shell bank
19. Compliance officer
20. Independent testing compliance
21. Staff recruitment and training

PART V
OFFENCES

22. Offences

Schedules

PURSUANT to section 48 of the Money Laundering Prevention Act 2007, I, **TUI ATUA TUPUA TAMASESE EFI**, Head of State, acting on the advice of Cabinet, **MAKE** the following Regulations:-

DATED this …….. day of…….…….....…2009

……
(Tui Atua Tupua Tamasese Efi)
HEAD OF STATE

REGULATIONS

PART I
PRELIMINARY

1. Title and Commencement – (1) These Regulations may be cited as the Money Laundering Prevention Regulations 2009.

(2) These Regulations commence in whole or in part, on such day or days nominated by the Minister.

2. Interpretation – (1) In these Regulations, unless the context otherwise requires -

"customer due diligence" means the process of identifying and reviewing a customers identity as described in regulations 5 to 11;

"FATF" means the Financial Action Task Force.

"FIU" means the Financial Intelligence Unit.

"internationally recognised standards" includes the 40+9 Recommendations established by FATF.

"politically exposed person" means

(i) any person who is or has been entrusted with a prominent public function in a foreign country, including, but not limited to a Head of State or of government, a senior politician, a senior government, judicial or military official;

(ii) any person who is or has been an executive in a foreign country of a state-owned company; and

(iii) any person who is or has been a senior political party official in a foreign country, and shall include any immediate family member or close associate of such persons.

"the Act" means the Money Laundering Prevention Act 2007.

(2) All other terms shall have the same meaning as provided in the Act unless the context otherwise requires.

(3) In these Regulations, "supervisory authority" in section 45 of the Act, means the authority designated to the financial institution described in Schedule 1.

3. Application – These regulations apply to financial institutions as defined in the Act.

4. Verification of customer identity – For the purposes of section 16 of the Act, all provisions do not apply, except for subsection 1(c) to a customer or a person carrying on business of:

(a) an insurer for issue of a compulsory third party motor insurance policy where the premium paid per annum is less than $500;

(b) a money lender where the transaction or total loan for a customer is less than $500;

(c) a consumer credit provider, including financial leasing, hire purchase and similar credit, where the transaction, inclusive of credit provided, is less than $1,000; or

(d) a money services provider for business or activity of collecting, holding, exchanging or remitting funds or the value or money, or otherwise negotiating transfers of funds or the value of money, on behalf of other persons where the transaction is less than $500 and where such transaction is completed domestically within Samoa and does not involve any foreign currency.

PART II – CUSTOMER DUE DILIGENCE

5. Customers who are natural persons – (1) For customers who are natural persons, a financial institution must:

(a) identify the customer on the basis of at least one of the following documents including:
  (i) a valid birth certificate;
  (ii) a valid citizenship certificate;
  (iii) a valid driver's licence;
  (iv) an international travel document such as a current and valid passport or any other travel document;
  (v) any other evidence of identity as may be determined by the Unit.

(b) verify the identity of the customer using independently sourced documents, data, or information which must include two or more of the following:
  (i) recent bank statement or account statement issued by another financial institution reflecting the name and residential address of the person if the person previously transacted with a bank or financial institution and that bank or financial institution had confirmed the person's particulars;
  (ii) Tax Identification Number and acknowledgement from the Ministry for Revenue (Inland Revenue Division)

reflecting the name and residential address of the customer;

(iii) utility bills recently issued by Electric Power Corporation, SamoaTel, Samoa Water Authority and other agencies to the customer at the address provided;

(iv) municipal rates and taxes invoice reflecting the name and residential address of the customer;

(v) mortgage statement from another financial institution reflecting the name and residential address of the customer;

(vi) cellular phone account reflecting the name and residential address of the customer;

(vii) recent long-term or short-term insurance policy document issued by an insurance company and reflecting the name and residential address of the customer;

(viii) current motor vehicle licence or registration document reflecting the name and residential address of the customer;

(ix) current land or other property ownership title document reflecting the name and residential address of the customer;

(x) an identification card issued to a public employee;

(xi) an identification card issued to a student at a tertiary or technical education institution;

(xii) written verification by a referee reflecting the name and residential address of the customer;

(xiii) other evidence as determined (with the approval by the Unit) that is reasonably capable of verifying the identity of the customer; or

(xiv) such other document, data or information as may be specified by the relevant supervisory authority with the approval of the Unit.

(2) Where a customer is a non-resident, the financial institution, must require and conduct verification of the following documents:

(a) valid passport or any other international travel document issued by a foreign government or a recognized international organisation;
(b) valid work, business or other permit issued by the Samoa Immigration Division of the Ministry of Prime Minister and Cabinet;
(c) valid visa issued by the Samoan Immigration Division of the Ministry of Prime Minister and Cabinet;
(d) valid employment document issued by their employer; or
(e) valid student status document issued by an education institution in Samoa.

(3) For the purposes of sub-regulation (2), "non-resident" means:

(a) a person who is not a Samoan citizen;
(b) a person who is a Samoan citizen and is domiciled overseas with the intention of obtaining permanent residency there; or
(c) any other person as may be determined by the Unit for the purposes of the Act and these Regulations.

6. Customers who are legal persons – (1) For customers who are legal persons, entities or legal arrangements, a financial institution must obtain and verify:

(a) the customer's name and legal form, obtaining proof of incorporation or similar evidence of establishment or existence through:
  (i) a certificate of registration from the Registrar of Companies; or
  (ii) a trust instrument;
(b) the personal details, including personal details required in regulation 5(1), (2) and (3), of each member of the customer's controlling body, including its directors and senior management such as the chief executive officer;
(c) the legal provisions that set out the power to bind the customer including the memorandum and articles of association or trust instrument or other legal instruments;
(d) the legal provisions that authorize persons to act on behalf of the customer (such as a

resolution of the board of directors or statement of trustees on opening an account and conferring authority on those who may operate the account); and

(e) the identity of the natural person purporting to act on behalf of the customer, using reliable, independently sourced documents as provided in regulation 5(1), (2) and (3);

(f) where the legal person, entity or arrangement is a business, either for profit or otherwise, or engages in, the business licence from the relevant local authorities.

(2) The financial institution must take reasonable measures to understand and document the ownership and control structure of the customer. This includes identifying the natural person who ultimately owns or controls a legal person, entity or arrangement using reliable, independently sourced documents as provided in regulation 5(1), (2) and (3).

(3) Where the customer is a company, limited partnership, or similar arrangement, the financial institution must undertake identification and verification of the principal owner, which at a minimum includes identifying:

(a) each natural person who owns directly or indirectly 10 percent or more of the vote or value of an equity interest in the company, limited partnership, or similar arrangement;

(b) any person exercising effective control of the company, limited partnership or similar arrangement; and

(c) each natural person who exercises a signing authority on behalf of the company, limited partnership, or similar arrangement.

(4) Where the customer is a trust or similar arrangement, identification and verification must be made of the settlors, trustees, and beneficiaries whose vested interest is more than 10 percent or more than 10 percent of the value of trust.

(5) In determining indirect ownership of equity interests,

(a) an equity interest held by a company, limited partnership, or similar arrangement, and by a trust, is taken to be owned proportionately by

its shareholders, partners, or vested beneficiaries; and

(b) an equity interest held by a family member is taken to be owned, in its entirety by each family member including brothers and sisters, whether by the whole or half blood, spouse, ancestors, and lineal descendants.

(6) Where the customer is a non-profit organization, group or agency the financial institution must satisfy itself as to the legitimate purpose of the organization by reviewing its charter, constitution, or trust instrument.

7. Insurance – Where a person is a customer for life and investment-linked insurance, the financial institution must identify and verify each beneficiary under the policy using, independently sourced documents as provided in regulation 5(1), (2) and (3).

8. Non face to face customers – (1) For non face-to-face customers, additional procedures for identification and verification must be used and these may include but are not limited to:

(a) certification of documents presented;
(b) requisition of additional documents to complement those that are required for face-to-face customers;
(c) independent contact with the customer by the financial institution; and
(d) third party introduction.

9. Determination of person on whose behalf the Customer is acting – (1) A financial institution must take reasonable measures to determine if a customer is acting on behalf of any other person or persons including on behalf of a beneficial owner or a controller.

(2) If the financial institution determines that the customer is acting on behalf of another person or persons then it must obtain and verify the identity of the other person by using relevant information or data obtained from an independent source and independently sourced documents as provided in regulation 5(1), (2) and (3).

10. Delay in verification of customers – A financial institution may delay completion the customer verification process for a given category of customers if:

(a) the financial institution identifies the circumstances in which customer verification can be delayed and procedures to manage the risk concerning delayed customer verification are in place ;
(b) the financial institution ensures that verification occurs as soon as practicable afterwards;
(c) the delay is essential to maintaining the normal course of business; and
(d) the money laundering and financing of terrorism risks are effectively managed.

11. Reliance on Third Parties or Intermediaries – (1) A financial institution may rely on a third party or intermediary to perform the customer identification requirements of the Act as provided in this Regulation and guidelines issued by the relevant supervisory authority.

(2) A financial institution may rely upon another financial institution and non-financial institutions to perform customer identification requirements if the financial institution:

(a) is satisfied that the third party or intermediary is adequately regulated and supervised and has measures in place to comply with the customer identification requirements of the Act and these Regulations;
(b) is satisfied that the customer due diligence procedures of the third party or intermediary are as rigorous as those which the financial institution would have conducted itself for the customer;
(c) reaches a written agreement with the third party or intermediary to promptly verify the due diligence undertaken by the third party or intermediary at any stage; or
(d) is satisfied that the third party or intermediary will not be subject to any action that calls into question its execution of those policies, and is located in a jurisdiction that is effectively implementing internationally recognised standards for customer identification.

(3) Where a financial institution relies on a third party or intermediary, the financial institution must immediately

obtain from the third party or the intermediary the customer identification information required in these Regulations and the Act.

(4) A financial institution must take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the information will be made available without delay.

(5) A financial institution must not rely upon a third party or intermediary that the relevant supervisory authority or the Unit:

(a) has identified as not complying with customer identification and verification requirements comparable with the Act or these Regulations; or

(b) has reason to believe are not complying with such requirements.

(6) A financial institution must only rely upon certain other third parties or intermediaries as directed by the Unit.

(7) The ultimate responsibility for the implementation of the customer identification and verification requirements of the Act and these Regulations remains with the financial institution.

12. Ongoing Due Diligence – (1) A financial institution must on an ongoing basis, gather and maintain customer information and monitor transactions.

(2) As part of the monitoring system, a financial institution must:

(a) pay special attention to all complex, unusual or large transactions, or unusual pattern of transactions that have no visible economic or lawful purpose;

(b) pay special attention to business relations and transactions with persons in a country that does not have adequate systems in place to prevent or deter money laundering or the financing of terrorism; or

(c) pay special attention to electronic funds transfers that do not contain complete originator information; and

(d) examine as far as possible the background and purpose of such transaction and set forth their findings in writing; and

(e) determine if a suspicious transaction report must be filed.

(3) Where applicable to the size and nature of business of the financial institution, the monitoring system must be capable of identifying transactions that are:

(a) from sources or to recipients identified as being of questionable legitimacy;

(b) unusual in terms of:

(i) amount (for example by reference to predetermined limits for the customer in question or to comparative figures for similar customers);

(ii) type (for example international wire transfers for the customer in question);

(iii) numbers (for example high account activity in relation to the size of the balance of the customer in question); or

(iv) any other risk factor identified by the financial institution; and

(c) identified in writing by the Unit as being a transaction that the financial institution must monitor.

(4) For the purposes of determining whether a country has adequate systems in place to prevent or deter money laundering or the financing of terrorism, a financial institution must take into account any information available on whether the country adequately applies the internationally recognised standards, including by examining the reports and reviews prepared by the FATF, FATF-Style Regional Bodies, the International Monetary Fund, and the World Bank.

13. Ongoing monitoring of customers – (1) For the purposes of section 20 of the Act, a financial institution must create and maintain a customer profile for each customer of sufficient nature and detail to enable the financial institution to monitor the customer's transactions, apply enhanced customer due diligence and detect suspicious transactions.

(2) A customer profile must include:

(a) relevant information as to the normal and reasonable activity for particular types of customer taking into account the nature of the customer's business;

(b) a comprehensive picture of the customer's transactions;
(c) the source and legitimacy of the funds; and
(d) the overall relationship with the financial institution.

(3) A financial institution must implement internal controls and procedures that establish the general purpose, type, volume and value, and the origin and destination of funds involved in the transactions.

(4) Internal controls and procedures may include the following:
(a) measures required under Part II of these Regulations; and
(b) additional measures to ensure that the required information is obtained when a transaction is conducted by the customer.

(5) If a financial institution fails to ascertain the required information for the proposed transaction, the financial institution must:
(a) not proceed with the transaction unless directed to do so by the Unit; and
(b) report the attempted transaction to the Unit as a suspicious transaction under section 17 of the Act.

14. Enhanced customer due diligence for higher risk customers, business relationships, and transactions – (1) Where customers are classified as higher risk customers, a financial institution must undertake enhanced customer due diligence.

(2) Enhanced customer due diligence must include enhanced:
(a) scrutiny of customer's identity (including of the beneficial owner and controller);
(b) scrutiny of the source and legitimacy of funds;
(c) transaction monitoring; and
(d) customer profiling.

(3) Enhanced customer due diligence must be applied to higher risk customers, business relationships, and transactions as appropriate at each stage of the customer identification and verification process.

(4) A financial institution must have policies and procedures in place and must ensure the effective implementation of these measures to address any specific risks associated with non-face-to-face business relationships or transactions.

(5) A financial institution must undertake enhanced customer due diligence in relation to politically exposed persons as a category of high risk customer.

(6) A financial institution must put in place appropriate risk management systems to determine whether a customer, a potential customer or the beneficial owner is a politically exposed person.

(7) The relevant supervisory authority in consultation with the Unit may issue guidelines specifying what factors the financial institution must take into account when determining whether customers are of a higher risk.

(8) A financial institution must not enter into a business relationship with a higher risk customer unless a senior member of the financial institution's management has given approval in writing.

15. Simplified customer due diligence for Lower Risk Customers – (1) Where customers are classified as lower risk customers, a financial institution may apply a simplified customer due diligence procedure if:

(a) the risk of money laundering or financing of terrorism is lower;

(b) information on the identity of the customer and the beneficial owner of a customer is publicly available; or

(c) adequate checks and controls exist in Samoa, including:

(i) licensed and regulated financial institutions;

(ii) locally incorporated public companies that are subject to regulatory and disclosure requirements;

(iii) Samoan Government administrations or enterprises; and

(iv) local Governments and municipal councils;

(2) Simplified customer due diligence may include a lower level of:

(a) scrutiny for customer identification;
(b) scrutiny of the source and legitimacy of funds;
(c) scrutiny of the legitimacy of the recipient of funds;
(d) transaction monitoring; and
(e) customer profiling.

(3) Despite sub-regulations (1) and (2), at a minimum, the financial institution must obtain information about the name and address of the customer, and the legal form and nature of business and activity conducted by the customer.

(4) Despite sub-regulations (1) and (2), the financial institution must terminate simplified customer due diligence procedures when there is suspicion of money laundering or terrorist financing or conditions under regulation 14 apply.

PART III – REPORTING OF TRANSACTIONS AND INFORMATION

Policies and Procedures on Reporting Obligations

16. Originator Information Requirement – (1) For the purposes of section 21 of the Act, a financial institution carrying on the business or activity set out in clauses (1) and (6) of the Schedule to the Act must ensure that for all electronic funds transfer transactions and all other forms of fund transfers, the financial institution obtains and maintains full originator information and verifications.

(2) Full originator information includes:

(a) the name of the originator;
(b) the originator's bank and account number, or a unique reference number if there is no account number;
(c) the originator's address; and
(d) the amount of payment order.

(3) For cross-border electronic fund transfers and any other forms of fund transfers (including transactions using a credit or debit card to effect a fund transfer), the remitting financial institution must include full originator information in the message or payment form accompanying the funds transfer.

(4) For domestic fund transfers (including transactions using a credit or debit card as a payment system to effect a money transfer), the ordering financial institution must include either:

(a) full originator information in the message or payment form accompanying the electronic funds transfers and all other forms of funds transfers; or

(b) only the originator's account number or;

(c) where no account number exists, a unique identifier, within the message or payment form, providing that full originator information can be made available to the beneficiary financial institutions and to the Unit within three business days of receiving a request.

(5) If a cross-border electronic fund transfer and any other form of transfer is contained within a batch transfer and is sent by a financial institution, it may be treated as a domestic electronic fund transfer.

(6) The financial institution must ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing.

(7) Each intermediary in the payment chain must maintain all the required originator information with the accompanying fund transfer.

(8) A beneficiary financial institution must identify and scrutinize fund transfers that are not accompanied by complete originator information and constitute an enhanced risk of money laundering and financing of terrorism.

(9) For the purposes of sub-regulation (8) a financial institution must have at a minimum, the following procedures to address fund transfers that are not accompanied by complete originator information:

(a) a procedure for the financial institution to request the missing originator information from the financial institution sending the funds transfer;

(b) if the missing information is not forthcoming, a procedure for requesting the financial institution to consider whether, in all the circumstances, the absence of complete

originator information creates or contributes to suspicion about the fund transfer or a related transaction; and

(c) if the fund transfer is deemed to be suspicious, a procedure for reporting obligations by the requesting financial institution to the Unit under section 23 of the Act,

and the financial institution may decide not to accept the fund transfer.

(10) The relevant supervisory authority in consultation with the Unit shall issue guidelines in relation to the reporting of such transactions.

PART IV – INTERNAL PROCEDURES, POLICIES, SYSTEMS AND CONTROLS

17. Adoption and implementation of internal procedures, policies, systems, and controls – (1) A financial institution must adopt and implement effective programmes against money laundering and financing of terrorism including:

(a) written procedures, policies, systems, and controls to deter and prevent money laundering and financing of terrorism in accordance with this Regulation and the Act; and

(b) written internal procedures, policies, systems controls and compliance management arrangements, to ensure compliance with this Regulation and the Act.

(2) The programmes referred to in sub-regulation (1) must have regard to the risk of money laundering and financing of terrorism, the size and nature of business, and the types of products and services offered by the financial institution.

(3) A financial institution must have a system in place to identify customers whose activities pose a lower risk or a higher risk of money laundering or “high risk customers” or “low risk customers”.

18. Shell banks – (1) The internal control and policies of a financial institution must include measures to

guard and prohibit the financial institution against establishing relationship with a shell bank.

(2) For the purposes of sub-regulation (1), a "shell bank' means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

19. Compliance Officer – (1) For the purposes of section 31(1) of the Act, the compliance officer:

(a) must be at a senior level in the financial institution; and

(b) must provide the financial instution and the Unit with his or her contact information and any changes made thereafter.

(2) The financial institution must provide the compliance officer and where necessary any staff designated to him or her with:

(a) appropriate and adequate authority and responsibility to implement the requirements of the Act and these Regulations;

(b) the authority to act independently; and

(c) timely access to customer identification data, customer due diligence information, transaction records, and other relevant information.

(3) The compliance officer is responsible for ensuring compliance with the Act and these Regulations and must report to senior management above the compliance officer's next reporting level.

20. Independent testing of compliance – (1) A financial institution must require their auditor to test compliance (including sample testing) with the procedures, policies and controls required under Part IV of these Regulations, including:

(a) attestation of the overall integrity and effectiveness of the written procedures, policies, systems, and controls and technical compliance of the financial institution with the Act and this Regulation;

(b) transaction testing in all areas of the financial institution with emphasis on high-risk areas, products, and services to ensure that the

financial institution is complying with the Act and these Regulations;

(c) assessment of the employees' knowledge of procedures, policies, systems, and controls;

(d) assessment of the adequacy, accuracy, and completeness of employee training programmes; and

(e) assessment of the adequacy and effectiveness of financial institution's process for identifying and reporting suspicious transactions and activities, and other reporting requirements under the Act and these Regulations.

(2) The auditor may provide the supervisory authority with a copy of the report.

21. Staff Recruitment and Training – (1) A financial institution must put in place screening procedures to ensure high standards when hiring employees and to prevent the employment of persons convicted of offences involving fraud and dishonesty.

(2) Employee screening procedures must ensure that:

(a) employees have the high level of competence necessary for performing their duties;

(b) employees have appropriate ability and integrity to conduct the business activities of the financial institution;

(c) potential conflicts of interests are taken into account, including the financial background of the employee;

(d) fit and proper and code of conduct requirements are defined; and

(e) information on previous charges or convictions for offences involving fraud, dishonesty or other similar offences are made known to the financial institutions.

(3) A financial institution must establish ongoing employee training to ensure that employees are kept informed of new developments, including:

(a) information on current money laundering and financing of terrorism techniques, methods and trends;

(b) clear explanation of all aspects of anti-money laundering and combating the financing of terrorism laws and obligations; and

(c) requirements concerning customer due diligence and suspicious and other transaction reporting.

(4) The relevant supervisory authority in consultation with the Unit may issue guidelines in relation to the development and implementation of internal procedures, policies, controls and programs by financial institutions.

PART V – OFFENCES

22. Offences – (1) Any person or financial institution who contravenes or fails to comply with any provision of these Regulations commits an offence and is liable upon conviction to a fine not exceeding 100 penalty units or imprisonment for a term not exceeding 1 year, or both such fine and imprisonment.

Schedule 1

Relevant supervisory authority

For the purposes of section 45 of the Act, for each entity set out in first column of the schedule, the relevant supervisory authority of the entity shall be the authority set out in the second column.

	Financial institutions	**Relevant supervisory authority**
(a)	any financial institution regulated or supervised by the Central Bank of Samoa;	Central Bank of Samoa
(b)	any financial institution regulated by the Samoa International Finance Authority;	Samoa International Finance Authority
(c)	accountants licensed by the Samoan Institute of Accountants	Samoan Institute of Accountants
(d)	any other financial institution;	Financial Intelligent Unit