



Bank South Pacific

Fraud and Whistleblower Policy

DOCUMENT CONTROL TABLE

Title of Policy:	Fraud and Whistleblower
Level of Policy:	Group
Type of Policy	Operational Risk
Owner of Policy:	Group Head of Operational Risk

VERSION CONTROL TABLE

Version No.	Date issued / reviewed	Effective Date	Amendment description / review details
0.1	22 March 2010		New document
0.2	30 March 2010		Management Review
1.0	6 April 2010	6 April 2010	Approved by EXCO

TABLE OF CONTENTS

1. OVERVIEW	3
1.1 CONTEXT	3
1.2 PURPOSE.....	3
1.3 SCOPE.....	3
2. DEFINITIONS.....	3
2.1. FRAUD.....	3
2.1.1 <i>CORRUPT CONDUCT</i>	3
2.1.2 <i>CONSPIRACY</i>	3
2.1.3 <i>MALADMINISTRATION</i>	3
2.1.4 <i>SERIOUS AND SUBSTANTIAL WASTE</i>	4
2.1.5 <i>BREACHES OF ANY LAW OR INTERNAL POLICY</i>	4
2.1.6 <i>OTHER MISCONDUCT BEHAVIOUR</i>	4
2.2. FRAUD TYPES.....	4
2.2.1 <i>INTERNAL (EMPLOYEE)</i>	4
2.2.2. <i>EXTERNAL</i>	5
2.3 SERVICE PROVIDER.....	5
3. POLICY PRINCIPLES	5
4. POLICY REQUIREMENTS	5
4.1 GENERAL REQUIREMENTS	5
4.2 GENERAL MANAGERS AND DEPARTMENT HEADS.....	5
4.3 EMPLOYEES, TEMPORARY STAFF, CONTRACTORS AND SERVICE PROVIDERS.....	6
4.4 OPERATIONAL RISK	6
4.5 WHISTLEBLOWER.....	6
4.5.1 <i>REWARD</i>	6
4.5.2 <i>CONTACTS</i>	6
4.5.3 <i>NON DISCRIMINATION</i>	7
5. GOVERNANCE.....	7
5.1. POLICY REVIEW.....	7

1. OVERVIEW

1.1 Context

The Fraud and Whistleblower Policy ensures that risks associated with fraudulent activities are minimised.

1.2 Purpose

The purpose of the Policy is to:

- Define BSP's principles and mandatory requirements for the prevention of fraud.
- Create an environment where the staff feel free, confident and encouraged to reveal any serious concerns they may have about the conduct of employees at all levels in the Bank, rather than overlooking a problem or "blowing the whistle" outside the bank, without fear of victimisation, subsequent discrimination or being disadvantaged in any way.

1.3 Scope

The Policy applies to all businesses, including subsidiaries and joint ventures where BSP has a controlling interest. It is applicable to all directors, employees, temporary staff, contractors and service providers.

2. DEFINITIONS

2.1. Fraud

Is the taking or obtaining by deception, money or any other benefit from the Bank when not entitled to the benefit; or attempting to do so and includes evading a liability to the Bank. Fraud includes, but is not limited to, offences involving dishonest or deceitful conduct with intent to obtain some financial advantage or property of another.

2.1.1 *Corrupt conduct*

Is when someone carries out their duties dishonestly or unfairly, breaches customer trust, misuses BSP information or resources, or becomes involved in matters such as bribery, fraud or violence.

2.1.2 *Conspiracy*

Is any conduct between two or more BSP employees or a BSP employee and an external party to do an unlawful act, or to commit an unlawful act by unlawful means.

2.1.3 *Maladministration*

Is conduct that involves action or inaction of a serious nature that is unlawful, against bank policies, unreasonable, unjust, oppressive, discriminatory, or is based on improper motives.

2.1.4 *Serious and substantial waste*

Is the loss or waste of the Bank's funds or resources.

2.1.5 *Breaches of any law or internal policy*

A material or systemic breach of any applicable law, regulation, code, license or internal policy.

2.1.6 *Other misconduct behaviour*

Misconduct, in these circumstances, may include, but is not limited to:

- Unacceptable practices
- Irregularities or conduct of an offensive nature
- Breach of PNG laws, including non-compliance
- Misrepresentation of facts
- Decisions made, and actions taken, outside established BSP policies and procedures
- Abuse of delegated authority
- Misuse of bank assets
- Disclosure of confidential information
- Health and safety risks including risks to the public and employees
- Unauthorised use of Bank assets
- Sexual harassment, or physical or sexual abuse of employees, customers and suppliers
- Unethical conduct
- Serious failure to comply with appropriate professional standards
- Abuse of power, or use of the Bank's powers and authority, for any unauthorised use, or personal gain
- Breach of code of conduct
- Deliberate breach or misrepresentation of facts, including misreporting to statutory reporting authorities
- Deliberate breach of approved Bank policy

2.2. Fraud Types

2.2.1 *Internal (employee)*

Employees, temporary staff, contractors or service providers who commit fraud against BSP or its customers. This also includes employees who issue or make misleading financial statements with the intent to deceive the investing public and the external auditor; or engage in bribes, kickbacks, influence payments and illegal or immoral schemes for their benefit or who conspires to commit same with one or more persons.

2.2.2. External

Customers or parties not employed by BSP who commit fraud against BSP or its customers.

2.3 Service Provider

Persons, contractors or organisations which provide services to BSP under written business arrangements, non-disclosure and contractual agreements.

3. POLICY PRINCIPLES

The principles set the underlying intentions from which the following mandatory requirements, and associated documents, are derived.

- Fraud risks should be managed in accordance with the following requirements:
 - BSP's Operational Risk Management Framework;
 - BSP's Code of Ethics;
 - BSP's Code of Conduct;
 - BSP's Occupational Health, Safety and Welfare; and
 - BSP's Network Usage Agreement.
- Fraud risks should be managed at a level in line with business objectives.
- Policies and standards related to fraud must be set and managed at appropriate levels.

4. POLICY REQUIREMENTS

4.1 General Requirements

- Fraud risk must be managed by staff members at all levels;
- BSP has Zero Tolerance for any form of fraudulent, corrupt or unethical behaviours by employees, contractors or service providers;

4.2 General Managers and Department Heads

- Must identify and assess fraud risks and take remedial actions where appropriate.
- Must implement and maintain adequate controls to address fraud and misconduct behaviours.
- Must implement and maintain adequate fraud measures to protect all products and services reliant on BSP's assets from unauthorised access, disruption and degradation.
- Must establish procedures for monitoring implementation of, and adherence to the Fraud and Whistleblower Policy;
- Must record all instances of non adherence to the Policy, and report to Group Head of Operational Risk.

4.3 Employees, Temporary Staff, Contractors and Service Providers

- Must ensure that they are aware of their fraud prevention responsibilities and obligations.
- Must adhere to the relevant fraud standards, guidelines and procedures.

4.4 Operational Risk

The Group Head of Operational Risk will:

- Develop and/or approve the underlying fraud standards, guidelines and procedures.
- Identify all operational risks (including fraud) within the Bank and report them accordingly to the Executive Committee and/or Board Audit Risk and Compliance Committee (BARCC).
- Coordinate the management of fraud risks to ensure that they are addressed across all areas of BSP in the most effective and efficient manner.
- Coordinate with Security Services and/or Internal Audit on internal and external fraud investigations.
- Ensure that all reported cases of fraud or unethical behaviour are treated with confidentiality and integrity.
- Perform a periodic review of the Fraud and Whistleblower Policy, taking into account reported incidents, instances of non adherence, emerging threats, risks and best practice.

4.5 Whistleblower

Employees are encouraged to report to management when they believe someone may be doing the wrong thing.

4.5.1 Reward

Safeguarding the human and material assets of BSP is a moral responsibility shared by all our employees and customers. Recognising that fraud causes a financial loss to the Bank, BSP will exercise its discretion in rewarding whistleblowers who have provided information that successfully prevents a fraud or helps identify those who have committed a fraud.

4.5.2 Contacts

The Bank has arrangements in place to receive phone calls and/or e-mails concerning suspected violations or wrongdoings. Anonymous reporting also can be made by using any of the following methods:

- Employee Hotline: 302 5288
 - Email: dbalchin@bsp.com.pg
- or
- Employee Hotline: 323-2154 ext. 203
 - Email: mgore@bsp.com.pg

4.5.3 Non Discrimination

No discriminatory action will be taken against any employee, who in good faith, reports a suspected violation of this policy or participates, in any subsequent investigation by the Bank.

“In good faith” means you genuinely believe wrongdoing has occurred.

Deliberately making a false report about an employee’s behaviour is a breach of this policy.

All such reports will also be investigated confidentially, consistent with a thorough and complete investigation, and remedied as appropriate.

A separate Fraud and Whistleblower operating procedure has been developed to support this policy (refer Appendix 1).

5. GOVERNANCE

5.1. Policy review

The Group Head of Operational Risk will conduct a periodic review of the Fraud and Whistleblower Policy which will take into account business experience in implementing the policy and industry practice.

When reviewed, factors including, but not limited to the following should be considered:

- Matters reported to EXCO and/or BARCC: operational losses, significant control weaknesses and audit issues;
- Amendments to regulatory requirements/guidelines/standards;
- Industry events; and
- Development and release of enhanced monitoring mechanisms.