



Fraud and Whistleblower Policy

March 2021

DOCUMENT CONTROL TABLE

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

VERSION CONTROL TABLE

Version No.	Date issued / reviewed	Amendment description / review details
0.1	22 March 2010	New document
0.2	30 March 2010	Management Review
1.0	6 April 2010	Approved by EXCO
1.1	23 October 2013	Management Review
1.2	7 November 2013	Approved by ORC
1.2	21 November 2013	Approved by BRCC
1.3	29 May 2017	Endorsed by ORC
1.3	13 July 2017	Approved by BRCC
1.4	December 2019	Review and update of document
1.4	14 February 2020	Approved by GCRO
1.5	29 January 2021	Approved by GCRO
1.6	25 March 2021	Amendment to comply with the ASX listing rules

TABLE OF CONTENTS

1. Overview	4
1.1 Context.....	4
1.2 Purpose.....	4
1.3 Scope.....	4
2. Definitions.....	4
2.1. Fraud.....	4
2.1.1 <i>Corrupt conduct</i>	4
2.1.2 <i>Conspiracy</i>	5
2.1.3 <i>Maladministration</i>	5
2.1.4 <i>Serious and substantial waste</i>	5
2.1.5 <i>Breaches of any law or internal policy</i>	5
2.1.6 <i>Other misconduct behaviour</i>	5
2.2. Fraud Types	6
2.2.1 <i>Internal (employee)</i>	6
2.2.2. <i>External</i>	6
2.3 Service Provider	6
3. Policy Principles.....	6
4. Policy Requirements	6
4.1 General Requirements	6
4.2 General Managers/Country Managers and Department Heads	<u>76</u>
4.3 Employees	7
4.4 Operational Risk.....	7
4.5 Whistleblower.....	7
4.5.1 <i>Reward</i>	7
4.5.2 <i>Contacts</i>	<u>87</u>
4.5.3 <i>Non Discrimination</i>	10
5. Reporting of a Whistleblower Complaint to the Board (Chair) or the Regulator. 10	
5.1. Reporting to the Chair	10
5.2. Reporting to BPNG (serious prudential concerns)	10
6. Governance	11
6.1. Policy review	11

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 BSP, rather than overlooking a problem or "blowing the whistle" outside BSP, without fear of victimisation, subsequent discrimination or being disadvantaged in any way.
- Ensure that all staff are aware that they will be held accountable for any actions or activities they undertake that is not in line with BSP's policies and guidelines.

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 Board Directors, employees, temporary staff, contractors and service providers.

2. DEFINITIONS

2.1. Fraud

Fraud conduct is:

- Taking or obtaining by deception, money or any other benefit from BSP when not entitled to the benefit; or
- Attempting to do so and includes evading a liability to BSP.

Fraud also 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*

Corrupt conduct is when a staff:

- 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.
- Is aware of corrupt dealings or practices but fails to report it to the appropriate stakeholder. This is seen as being negligent.

2.1.2 Conspiracy

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

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

2.1.4 Serious and substantial waste

Serious and substantial waste is the loss or waste of BSP'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 that do not reflect BSP's values
- Irregularities or conduct of an offensive nature (e.g. verbal abuse, physical threat)
- 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 or unauthorized use of BSP assets
- Disclosure of confidential information to unauthorised parties
- Health and safety risks including risks to the public and employees
- Sexual harassment, or physical or sexual abuse of employees, customers and suppliers
- Unethical conduct (e.g., lying or providing false information)
- Serious failure to comply with appropriate professional standards
- Abuse of power, or use of BSP'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 BSP policy

2.2. Fraud Types

2.2.1 Internal (employee)

BSP 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 Conduct;
 - BSP's Occupational Health, Safety and Welfare; and
 - BSP's Information Security Policy
- 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/Country 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 protect all products and services reliant on BSP's assets from unauthorised access, disruption and degradation by implementing and maintaining effective fraud measures.
- 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 Head of Group Operational Risk.
- All material incidents reported under this Policy must be reported to the BSP Board of Directors or BSP Risk Committee.

4.3 Employees

- 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 Head of Group Operational Risk will:

- Develop and/or approve the underlying fraud standards, guidelines and procedures.
- Identify all operational risks (including fraud) within BSP and report them accordingly to the Executive Committee and/or Board Risk Committee (BRC).
- 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 is in breach of BSP's policies, procedures and values.

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 BSP, and will exercise its discretion in rewarding whistleblowers that have provided information that successfully prevents a fraud or helps identify those who have committed a fraud.

4.5.2 Contacts

BSP has arrangements in place to receive phone calls and/or e-mails concerning suspected violations or wrongdoings. Anonymous reporting also can be via telephone or email to the following designated contacts:

In PNG:

Designated Contact: Mike Hallinan, Group Chief Risk Officer

- Employee Hotline: +675 305 6709
- Email: mhallinan@bsp.com.pg

or

Designated Contact: Carl Nuyda, Head of Group Operational Risk

- Employee Hotline: +675 305 6202
- Email: cnuyda@bsp.com.pg

or

Designated Contact: Rachele Roxas, Head of Group Internal Audit

- Employee Hotline: +675 305 6241
- Email: rroxas@bsp.com.pg

In Fiji:

Designated Contact: Haroon Ali, Country Manager

- Employee Hotline: +679 323 4867
- Email: hali@bsp.com.fj

or

Designated Contact: Michael Nacola, Managing Director, BSP Life

- Employee Hotline: +679 326 1777
- Email: mnacola@bsplife.com.fj

or

Designated Contact: Esala Halafi, Head of Operational Risk

- Employee Hotline: +679 323 4952
- Email: ehalafi@bsp.com.fj

In Solomon Islands:

Designated Contact: David Anderson, Country Manager

- Employee Hotline: +677 23 022
- Email: danderson@bsp.com.sb

or

Designated Contact: Lucy Bonunga, Operational Risk Manager

- Employee Hotline: +677 21 874

- Email: ibonunga@bsp.com.sb

In Tonga:

Designated Contact: Marcellina Rose Wolfgramm Haapai, Country Manager

- Employee Hotline: +676 20 807
- Email: MWolfgrammHaapai@bsp.com.pg

or

Designated Contact: Alvina Manu, Operational Risk Manager

- Employee Hotline: + 676 20 800 Ext 6129
- Email: amanu@bsp.com.pg

In Samoa:

Designated Contact: Maryann Lameko-Vaai, Country Manager

- Employee Hotline: +685 66 115
- Email: mlameko-Vaai@bsp.com.pg

or

Designated Contact: Peti Leiataua, Operational Risk Manager

- Employee Hotline: +685 66 129
- Email: pleiataua@bsp.com.pg

In Cook Islands:

Designated Contact: David Street, Country Manager

- Employee Hotline: +682 22 829
- Email: dstreet@bsp.com.pg

Designated Contact: Grace Tangata, Operational Risk Manager

- Employee Hotline: +682 22 014
- Email: gtangata@bsp.com.pg

In Vanuatu:

Designated Contact: Nik Regenvanu, Country Manager

- Employee Hotline: +678 28 630
- Email: nregenvanu@bsp.com.pg

or

Designated Contact: Edmond Williamson, Operational Risk Manager

- Employee Hotline: +678 28668
- Email: ewilliamson@bsp.com.pg

In Cambodia:

Designated Contact: Choeun Buo, Country Manager

- Employee Hotline: (Tel) + 855 (0) 23 211 011 (mobile) + 855 (0) 77 73 63 22
- Email: Choeun.Buo@rmagroup.net

In Lao:

Designated Contact: Viengsavanh Danchampa, Credit & Operational Manager

- Employee Hotline: (Tel) + 856 (0) 21 255501 (mobile) + 856 (0) 20 22210649
- Email: Viengsavanh.d@rmagroup.net

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 BSP.

“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 also been developed and maintained by Operational Risk to support this policy.

5. Reporting of a Whistleblower Complaint to the Board (Chair) or the Regulator

5.1. Reporting to the Chair

a) Employees to communicate illegal, unethical or questionable practices to higher levels including, the Chair, or the Chair of the Audit Committee or Audit and Risk Committee (in this instance it is the Board Risk Committee).

b) If there are serious prudential concerns, the Chair must report promptly to the BPNG.

5.2. Reporting to BPNG (serious prudential concerns)

a) Where the illegal, unethical or questionable practices relate to the Chair or Senior Management, the policy must provide that the employee may communicate the concerns directly to BPNG.

6. Governance

6.1. Policy review

The Head of Group 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 BRC: operational losses, significant control weaknesses and audit issues;
- Amendments to regulatory requirements/guidelines/standards;
- Industry events; and
- Development and release of enhanced monitoring mechanisms.