Objective

Suncorp is committed to operating with high standards of ethical behaviour. We expect our people to always behave in a manner that is consistent with our values and code of conduct to protect our customers, shareholders and communities from the reputational, regulatory and social consequences of Financial Crime.

This Policy sets out Suncorp's minimum expectations towards Financial Crime risk management and ensures compliance with the applicable laws, regulations, and community expectations for the jurisdictions in which it operates. Suncorp understands the reputational, regulatory, and social consequences of failure to meet such laws, regulations, and community expectations.

Application

This Policy applies to Suncorp (as defined in the General Policy definitions and terms in Collibra) unless otherwise stated.

Where Suncorp relies on third parties to perform services on the organisation's behalf, Suncorp will ensure that these third parties satisfy the same or equivalent requirements of this Policy as applicable.

Policy Statements

- Suncorp maintains robust practices to identify, manage and mitigate Financial Crime risks and obligations proportionate to the level of risk of its business operations;
- Suncorp has appropriately skilled and experienced specialists engaged to implement prevention, detection and response strategies for Financial Crime;
- Suncorp has Internal Fraud (including Bribery & Corruption), External Fraud, and Sanctions awareness and prevention training that promotes a culture of speaking up and supports incident identification and reporting;
- Internal Fraud, Bribery and Corruption including Facilitation Payments is prohibited and Suncorp has a zero-tolerance approach;
- Where an Employee has a reasonable belief or suspicion that Internal Fraud, Bribery or Corruption has occurred, it must be reported to their leader, Group Internal Fraud or via Suncorp's Whistleblower service;
- Suncorp has central registers[1] with accurate records of financial and non-financial information to enable timely identification and disclosure of incidents to regulators, responses to law enforcement and/or regulator enquiries and to demonstrate the steps taken to mitigate bribery & corruption risks;
- Suncorp maintains procedures that assess Sanctions risk and prescribe reasonable precautions and due diligence to manage obligations and avoid contravening relevant sanctions laws; and
- Suncorp assesses the applicability of AML CTF obligations to its existing and new business activities. Where business activities are subject to AML CTF obligations, the Chief Risk Officer must approve the new business activity and Suncorp must maintain systems and controls to meet the obligations.

[1] The required information can be maintained using central registers recording information on conflicts of interest, risk assessments, due diligence, audits, external reviews, corporate expense, donations (political/charitable), sponsorships, etc.

Accountabilities

The following are specified accountabilities not otherwise set out in this policy:

Business CEOs or equivalent

- Implement the financial crime prevention policy, framework and associated standards within the remit of the Function;
- Refer suspected or alleged Internal Fraud or Bribery & Corruption to Group Internal Fraud;
  - In Australia, suspected or alleged External Fraud, or Sanctions exposure is referred to Fraud & Intelligence; and
  - In New Zealand, suspected or alleged External Fraud is referred to Fraud Detection or claims related allegations to Major Loss & Investigations, and suspected or alleged Sanctions exposure is referred to Compliance, Regulatory & Assurance.

Group Internal Fraud (People, Legal & Corporate Services)

- Investigate all suspected and alleged Internal Fraud, including Bribery and Corruption; and
- Refer Internal Fraud including Bribery and Corruption matters to law enforcement agencies where evidence of illegality is identified.

Financial Crime Compliance (Risk & Advocacy)

- Develop, maintain and review the financial crime prevention policy, framework and associated standards,
- Report sanctions breaches to the relevant regulator where appropriate, and
- Conduct 2LOD oversight in relation to financial crime risk and obligation management.

Fraud & Intelligence (Technology & Operations)

- Investigate and report External Fraud and Sanctions matters referred by the Functions or identified through detection practices; and
- Refer External Fraud matters to law enforcement agencies as appropriate where evidence of illegality is identified and notify the respective Function CEO of financial crime matters that have been referred.

Fraud Detection (Suncorp New Zealand)

- Investigate External Fraud matters identified through detection practices and refer to the relevant business area where appropriate; and
- Refer External Fraud matters to law enforcement agencies as appropriate where evidence of illegality is identified and notify the respective Function CEO of financial crime matters that have been referred.

Compliance, Regulatory & Assurance (Suncorp New Zealand)

- Investigate Sanctions matters referred by Suncorp New Zealand or identified through detection practices; and
- Report New Zealand sanctions breaches to the relevant regulator where appropriate.

Major Loss & Investigations (Suncorp New Zealand)

- Investigate external claims fraud matters referred by Analytics & Fraud Detection team or identified through detection practices.

Policy Exemptions

No exemptions apply to this Policy. Country level policies should only be developed where there are local legal or regulatory requirements and approval should be sought from Head of Compliance.

Policy Breaches

All Policy breaches must be managed in accordance with the Incident Management Standard and the Breach Assessment and Reporting Standard or SNZ Breach Assessment Standard, with the Policy Owner notified. A breach of this Policy may result in disciplinary action (including termination of employment or engagement), financial loss, and/or legal or regulatory action.

Key Terms

Unless otherwise defined in this Policy, commonly used terms and phrases are defined in the General Policy definitions and terms in Collibra. Conflicts of Interest (COI) terms and phrases are defined in the COI glossary in Collibra.

Bribery	The offering, promising, giving, accepting, or soliciting of any undue advantage of any value (financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person (including a “Public Official”) acting or refraining from acting in relation to the performance of that person’s duties. Note: Bribery is a subset of Corruption, all instances of Bribery will constitute Corruption, but not all instances of Corruption will constitute Bribery.
Bribery and Corruption	Dishonest activity in which a person associated with Suncorp (e.g., director, executive, manager, employee or contractor) acts contrary to the interests of Suncorp and abuses their position of trust in order to achieve personal advantage or advantage for another person or organisation. This can also involve corrupt conduct by Suncorp, or a person purporting to act on behalf of and in the interests of Suncorp, in order to secure some form of improper advantage for Suncorp either directly or indirectly. Note While conduct must be dishonest for it to meet the definition of Corruption, the conduct does not necessarily represent a breach of the law
External Fraud	is any activity that relies on deception to achieve an unfair or unlawful gain, or to deprive a victim of a legal right and committed or attempted by a third party outside the organisation such as vendors, suppliers, customers, or competitors and includes scams.
Facilitation Payment	is an illegal or unofficial payment (usually of nominal value) paid to an official for the sole or predominant purpose of expediting a minor routine action.
Financial Crime	Includes Fraud, Bribery and Corruption, Money Laundering and Terrorism Financing, Scams and Sanctions.

Internal Fraud	is any activity that relies on deception to achieve an unfair or unlawful gain, or to deprive a victim of a legal right and committed or attempted by at least one internal party within an organisation such as an employee.
Money Laundering	is the process by which criminals attempt to hidden and disguise the true origin and ownership of the proceeds of their criminal activities and thereby have these funds enter the normal economy to make it seem as if the money has been obtained legitimately.
Sanctions	Measures developed and imposed by governments and international organisations to address situations of international concern by restricting activities and conduct that relate to countries and regions, themes of conduct, goods and services, or persons, groups, and entities. Situations of international concern can include repression of human rights, proliferation of weapons of mass destruction, internal or international armed conflict, terrorism, arms trafficking, narco-trafficking, and financial crimes such as bribery, corruption, and cybercrime. Key legislative obligations are set out in the Australian Autonomous Sanctions Act 2011, the New Zealand Russia Sanctions Act 2022, and the United Nations Security Council sanctions regime.
Scam	is a type of external fraud where customers are deceived by another party to authorise an action that, if successful, would cause loss or harm to the customer.
Terrorism Financing	is the act of unlawfully and willingly providing or collecting funds (whether directly or indirectly) with the intention that they should be used or, in the knowledge that they are to be used, in support of an act of terrorism.