Fraud Risk Management Policy

Risk Policy | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	Fraud Risk Management Policy
Document type	Risk Policy
Jurisdiction	Global
Owner	Chief Risk Officer
Approved by	Board Risk Committee
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

This Policy establishes the Company's requirements for managing the risk of internal and external fraud, including scams perpetrated against the Company's customers. It defines the fraud taxonomy the Company uses, the prevention, detection, investigation, recovery and reporting controls that must operate, and the accountabilities of the Board, management and all staff for fraud risk.

Fraud risk is a material operational risk. Uncontrolled, it causes direct financial loss, customer harm, regulatory breach and lasting reputational damage. This Policy exists to ensure that fraud risk is managed within the Board-approved risk appetite through a coherent control framework spanning all three lines of the three lines model, consistent with the COSO Fraud Risk Management Guide, the ACFE's fraud risk management frameworks and the BCBS Principles for the Sound Management of Operational Risk.

This Policy is approved by the Board Risk Committee, is owned by the Chief Risk Officer, and forms part of the Company's risk management framework. It must be read alongside the Operational Risk Policy, the AML/CFT Program, the Whistleblower Protection Policy, the Anti-Bribery and Corruption Policy, the Information Technology Security Policy and the Issues and Incident Management Policy.

2. Scope

This Policy applies to the Company and all of its controlled entities, and to all directors, employees, contractors, secondees and agency staff (collectively, staff). Relevant obligations extend to material service providers and other third parties acting for the Company, and must be reflected in contractual terms under the Company's third-party risk management arrangements.

The Policy covers all products, channels and business activities, including lending, deposits, payments, cards, digital channels, branches, contact centres and corporate functions such as procurement, payroll and finance. It covers fraud committed against the Company, fraud committed against customers through the Company's products and channels (including scams), and fraud committed by staff or third parties using the Company's position, systems or information.

Bribery and corruption are addressed in detail in the Anti-Bribery and Corruption Policy; money laundering and terrorism financing controls are addressed in the AML/CFT Program. Where conduct engages more than one policy, all applicable requirements apply, and the investigation protocol in this Policy governs the fraud elements.

Jurisdictional application. This Policy states international best practice, anchored to the frameworks listed in the Regulatory Framework section. The Company must map the requirements of this Policy to the law of each jurisdiction in which it operates, including criminal law, reporting obligations, employment law and data protection law, and must document that mapping. Where applicable local

law imposes a stricter or additional requirement, local law prevails over this Policy.

3. Definitions

Term	Definition
Fraud	Any intentional act or omission designed to deceive others and thereby obtain a benefit or cause a loss, whether financial or non-financial. Fraud requires dishonest intent; carelessness, error or process failure without dishonest intent is not fraud, although it may constitute an operational risk event or a breach of another policy.
Internal fraud	Fraud, misappropriation of assets or circumvention of law, regulation or Company policy that involves at least one director, employee, contractor or secondee of the Company, whether acting alone or in collusion with external parties. Corresponds to the internal fraud event type in the Basel operational risk event taxonomy.
External fraud	Fraud perpetrated against the Company or its customers by a third party with no internal involvement, including application fraud, identity takeover, scams, card and transaction fraud and cyber-enabled fraud. Corresponds to the external fraud event type in the Basel operational risk event taxonomy.
Corruption	The misuse or abuse of entrusted power, position, trust or information for private gain or advantage, whether for the person concerned or another party, including bribery, kickbacks, collusive tendering, improper conflicts of interest and conduct that confers an improper advantage on, or disadvantages, another person or entity.
Scam	A dishonest invitation, request, notification or offer designed to deceive a person into authorising a payment, disclosing credentials or providing personal information, resulting in loss or attempted loss. In a scam the customer is deceived into acting; in unauthorised fraud the transaction occurs without the customer's authority.
Authorised push payment (APP) fraud	A scam in which a customer is deceived

	into authorising a payment from their own account to an account controlled by a criminal, typically via investment, romance, invoice-redirection, remote-access or impersonation scams.
Application fraud	The use of false, stolen or synthetic identity information, or materially false statements, to obtain a product, facility or service from the Company. Includes both first-party fraud (a genuine identity misrepresenting intent or circumstances) and third-party fraud (use of another person's identity).
Identity takeover	The unauthorised use of a genuine customer's identity or credentials to gain control of an existing account or to open new facilities, including account takeover following phishing, SIM-swap, malware or data compromise.
Mule account	An account used to receive, hold or pass on the proceeds of fraud or scams, whether the account holder is complicit, recruited or themselves deceived.
Account name verification	A service (in some markets called Confirmation of Payee) that checks the account name entered by a payer against the name held by the receiving institution before a payment is made, and returns a match, partial match or no-match result to the payer.
Fraud triangle	The model, reflected in the COSO Fraud Risk Management Guide, holding that fraud typically requires the coincidence of pressure or incentive, opportunity, and rationalisation; anti-fraud controls are designed principally to remove opportunity and to detect the exploitation of it.
Financial Intelligence Unit (FIU)	The national agency in each jurisdiction in which the Company operates that acts as the central authority for receiving, analysing and disseminating suspicious transaction reports and other information relevant to money laundering, associated predicate offences, terrorism financing and proliferation financing, consistent with the FATF Recommendations.
Suspicious Transaction Report (STR)	A report submitted to the FIU, however styled in the relevant jurisdiction and including a suspicious activity report (SAR), where the Company suspects or

	has reasonable grounds to suspect that funds or activity are the proceeds of criminal conduct, including fraud, or are related to terrorism or proliferation financing, consistent with FATF Recommendation 20.
Operational Risk Event	A discrete occurrence arising from inadequate or failed internal processes, people or systems, or from external events, that has resulted or could have resulted in a financial loss, gain or near miss, or in a non-financial impact such as customer detriment, regulatory breach, data loss or service disruption.
Fraud risk assessment (FRA)	A structured assessment, consistent with Principle 2 of the COSO Fraud Risk Management Guide, that identifies the Company's fraud risks, evaluates inherent likelihood and impact, maps existing controls, rates residual risk and assigns treatment actions.
Whistleblower	A person who reports, or is entitled to report, suspected wrongdoing concerning the Company — including fraud, corruption or other misconduct — through internal or protected reporting channels, an independent reporting service or a competent authority, and who is entitled to confidentiality and protection from retaliation under applicable local law.
Three Lines Model	The Company's accountability model, based on the Institute of Internal Auditors' Three Lines Model, in which business and support units own and manage risk (first line), the risk and compliance functions set frameworks and provide oversight and challenge (second line), and Internal Audit provides independent assurance (third line).

4. Regulatory Framework

The key legislation, regulations and standards relevant to this document include (as amended from time to time):

Instrument / Standard	Relevance
COSO Fraud Risk Management Guide (2nd edition, 2023, with the ACFE)	Primary framework for this Policy: fraud risk governance, fraud risk assessment, preventive and detective control activities, investigation and corrective action, and

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.

finance-policies.com