Enterprise Fraud Framework

Accountable Executive:	Chief Risk Officer
Date Approved:	10 March 2020
Date Effective:	10 March 2020

Contents

1. Executive Summary

1.1. Purpose

Australia Post Group (APG) is defined as the Australian Postal Corporation and its subsidiaries. This includes employees, contractors, consultants, licensees, agents and other third parties performing services for, or on behalf of, APG.

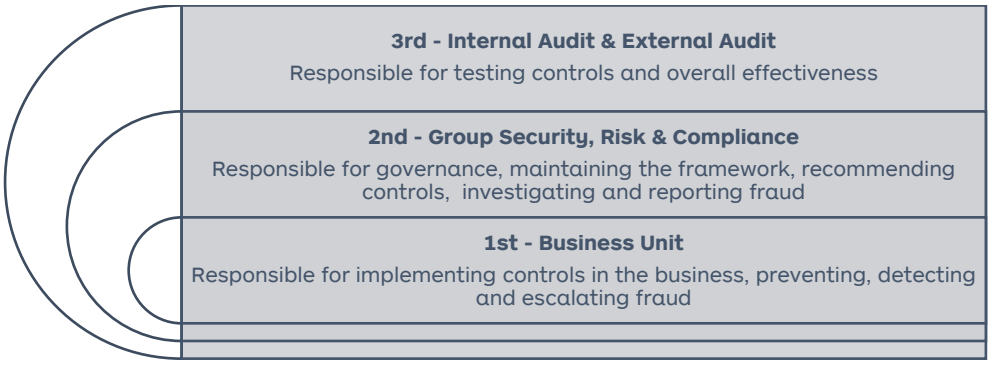
This framework:

- Provides an understanding of what fraud is and how it can impact APG
- Applies to all staff
- Describes the roles, responsibilities and accountabilities of all staff and business units within APG regarding the prevention, detection, investigation and reporting of fraud
- Aligns APG with best business practice in accordance of the *AS 8001:2008 Fraud Control*

1.2. Introduction

APG's values underpin everything we do, the services we deliver, the products we provide and how we behave and communicate with each other and our customers. The Enterprise Fraud Framework will ensure the organisation continues to act and work with integrity and comply with applicable laws, regulations, codes, policies and procedures. This document will also be a guide for the organisation to deliver effective fraud strategies in line with the Group Fraud Policy.

APG uses the 'three Lines of defence' model to protect the organisation from the impact of fraud.



1.3. Definition of Fraud

Any intentional act by one or more individuals (internal and external), involving the use of deception or misrepresentation to obtain an unlawful advantage to the detriment of APG.

Fraud against APG may include, but is not limited to:

- Misappropriation of funds, securities, stock, supplies or other assets including use of assets for private purposes
- Planning or causing a loss to or creating a liability for Australia Post by deception
- Impropriety in the handling or reporting of money or financial records
- False invoicing for goods or services never rendered or backdating agreements
- Create or maintain artificial prices
- Submission of exaggerated or wholly fictitious accident, harassment or injury claims
- Entering or engaging in fictitious transactions
- Misuse of entitlements

APG has two classifications of fraud:

- **INTERNAL FRAUD** is where fraud against APG is committed by its employees or contractors and there is a direct impact to the organisation
- **EXTERNAL FRAUD** is where fraud against APG is committed by an external party and there is a direct impact to the organisation or, where APG is used by others as the vehicle to commit fraudulent or criminal acts (e.g. mail redirections)

1.4. Statement of the APG's attitude toward Fraud

APG does not tolerate fraud, is committed to the highest levels of integrity and expects ethical and lawful behaviour in all business practices.

APG will consider and assess all reports of internal and external suspected or detected fraud and make the appropriate determinations on the right courses of action. This may include disciplinary, civil, legal or any other action deemed appropriate.

1.5. Code of conduct

This framework is consistent with APG's 'Our Ethics' policy which sets the standards of conduct and behaviour for the organisation.

This framework applies to all business units and includes, but is not limited to, employees, consultants, contractors, franchisees, service providers and business partners, who are all required to acknowledge compliance with Our Ethics, and the Group Fraud Policy.

1.6. Related policies and documents

The following plans, policies, procedures and documents are established in APG and should be read in conjunction with this framework:

- Our Ethics
- Group Fraud Policy
- Group Whistleblower Policy
- Group Risk Management Policy
- Anti-Bribery and Corruption Policy

1.7. Related legislation and guidelines

The framework draws on, and is consistent with the following standards, legislation and guidelines:

- The Australian Postal Corporation Act 1989
- The Public Governance, Performance and Accountability Act 2013 (PGPA) and the PGPA Rule 2014
- Australian Standard on Fraud and Corruption Control (AS8001:2008)
- The Australian Government Investigation Standards (AGIS) 2011
- Criminal Code Act 1995, which sets out criminal offences against the Commonwealth

1.8. Roles and accountabilities for Fraud control

Roles and responsibilities defined in this framework include those roles and responsibilities detailed in the Group Risk Management Framework.

APG is a Government Business Enterprise bound by Section 10 of the PGPA. Under this act, APG must prevent, detect and deal with fraud by:

- Conducting fraud risk assessments
- Developing, implementing and maintaining fraud control plans
- Having an appropriate mechanism for preventing fraud through awareness, training and planning
- Having an appropriate mechanism for detecting incidents of suspected fraud, including a process for employees to report suspected fraud confidentially
- Have an appropriate mechanism for investigating incidents of fraud
- Having an appropriate mechanism for recording and reporting incidents of fraud

Board of Directors - In accordance with the Board Charter, the role of the APG Board is to decide the objectives, strategies and polices to ensure APG performs its functions in a manner that is proper and efficient. It is the Board's responsibility to ensure appropriate governance mechanisms and frameworks are in place and effective in their execution. The Board is accountable to the Shareholder Minister (under the PGPA) and must report on the implementation of governance frameworks, including fraud, in the Annual Report.

Board Audit and Risk Committee - A sub-committee established to assist the Board discharge its responsibilities under the Australia Post Corporation Act 1989 and the PGPA, particularly in relation to financial reporting, risk management and internal control. The Board Audit and Risk Committee also monitors compliance with relevant requirements of other laws and regulations. The Board Audit and Risk Committee oversees and reviews systems of internal control and risk management, including fraud risk.

Chief Risk Officer - Responsible for implementing and overseeing the Group Fraud Policy and this framework.

Group Security - Responsible for developing and maintaining the Enterprise Fraud Framework and will:

- Set the overall fraud strategy and framework for the organisation
- Manage the Group Fraud Policy and this framework to ensure they are consistent with the appropriate legislation, regulation and APG policies
- Ensure any significant fraud is reported and escalated as necessary
- Investigate significant alleged material fraud matters within the organisation
- Provide best-practice advice and assistance to the business
- Develop and implement fraud-related awareness and training for staff

Managers - Accountable for identifying and managing fraud risks associated with their businesses and activities. Managers are responsible for fostering an environment that makes fraud control a business as usual consideration for all employees. Managers are accountable for the development and implementation of a Fraud Control Plan to address identified fraud risks in their business areas.

Staff - It is the responsibility of all staff to minimise the possibility of fraud within the business. This includes managing fraud related risks relevant to their role, and ensuring the continued operation of controls to prevent fraud. All staff are required to immediately report any suspected or detected

fraudulent activity to their line manager or supervisor, Group Security or through the Whistleblower Hotline. All staff will undergo continuation training.

2. Planning and Resourcing

2.1. Enterprise Fraud Framework

This document will be reviewed at least every two years but a review can be triggered at any time by changes in the Australian Standard for Fraud and Corruption Control, by other legislative requirements, or by other operational requirements (as required).

Business units will apply appropriate resourcing to manage their own level of fraud risk.

2.2. Fraud Control Officer and accountabilities

The National Fraud and Security Risk Advisor, reporting to the Head of Security Operations, is responsible for developing, implementing and operationalising the fraud portfolio.

2.3. External assistance

At times of high workload or when specialised skills are required; external parties may be engaged to assist with conducting fraud risk assessments or the investigation of suspected fraud, including the use of forensic techniques.

Group Security may engage these services on an as needs basis with the appropriate authorisation. Costs associated with engaging external service providers is borne by the business unit where the work is necessary to be undertaken. The engagement of consultants greater than $100k requires the approval of the Group Chief Financial Officer.

2.4. Internal Audit in Fraud control

Internal Audit is the third line of defence which provides independent assurance over the effectiveness and efficiency of our control environment. It is the responsibility of Internal Audit to have sufficient knowledge to evaluate the risk of fraud and the way it is managed by the organisation. Internal Audit can conduct or assist in the investigation of suspected or detected fraudulent activities within APG in accordance with the Board Audit and Risk Committee endorsed Internal Audit Charter. If an internal auditor detects a fraud or identifies a potential fraud risk or exposure, they must then report this to Group Security and the Board Audit and Risk Committee.

3. Fraud Prevention

3.1. Implementing and maintaining an integrity framework

The Group Chief Executive Officer and Managing Director and the Executive Leadership Team are committed to ensuring an ethical and high-integrity workplace. APG does not tolerate fraud and senior management are responsible for conveying and promoting this message to staff.

3.2. Line management accountability for controlling Fraud

It is critical that front line management are aware of the impacts of fraud in their areas and are accountable for detecting, preventing and reporting fraud. Managers will be provided fraud awareness training so they understand their responsibilities. Failure to report fraud identified in their business may result in further action taken by their manager.

Managers are accountable for identifying and managing the fraud risks associated with their business objectives and strategic activities. Managers are responsible for fostering an environment that makes fraud control a responsibility for all employees, articulating clear standards and procedures to encourage deterrence of fraud, and the detection and reporting of fraud incidents. Managers are responsible for:

- Setting the tone at the top for the organisation by demonstrating and communicating that fraud is not tolerated, that any such behaviour is dealt with swiftly and decisively, and that genuine whistleblowers will not suffer retribution
- Implementing adequate internal controls
- Having primary responsibility for the identification of fraud
- Participating in fraud risk and control self-assessments as required
- Ensuring fraud training is completed

3.3. Employee responsibilities

APG employees are responsible for:

- Having a basic understanding of fraud in the context of their role
- Understanding their role within the internal control framework and when non-compliance of procedures may create an opportunity for fraud to occur or go undetected
- Avoidance of conflict of interest
- Reading, understanding and complying with regulatory obligations, policies and procedures relevant to their current workplace responsibilities, including the Group Fraud, Our Ethics and Whistleblower policies
- Completing all relevant fraud training programs

3.4. Fraud risk assessment

Fraud-related risks should be assessed by each business unit in accordance with the Group Risk Management Standard. Group Risk can facilitate these risk assessments and, where fraud risks are identified, support will be provided by the National Fraud and Security Risk Advisor.

A risk assessment that addresses fraud related risk will establish the level, nature, form and likelihood of fraud related risk exposures. Like any risk assessment process, assessments of fraud related risk must be conducted as an ongoing, iterative process. This will maximise the opportunity to identify and treat all fraud related risks. Consideration of risk factors should include both internal and external environments and should address all business processes.

Business units are to apply the Group Risk Management Standard to assess their fraud risks as part of their business risk management process, and must fully document the outcomes from the risk assessment process.

Risk assessment is a process of continuous improvement. When the risk assessment process begins, business units must attempt to gain an understanding of the various fraud scenarios that may occur.

Potential areas that should be considered in relation to fraud-related risk include:

- Information technology, information security, user access and the segregation of duties
- eCommerce, product and identity services, electronic service delivery and the internet
- Outsourced functions and funded service delivery programs
- Grants, funding agreements, and other payments or benefits programs
- Procurement, tendering processes, purchasing and contract management
- Retail services provided by Retail
- Invoicing, revenue collection and cash handling
- Use of business credit cards
- Travel and other common allowances
- Salaries and Payroll
- Property (including intellectual property) and other physical assets including physical security
- Supplier and vendor management

The outcome of the risk assessment process will be the development of fraud plans to further mitigate and manage identified fraud related risks.

3.5. Communication and awareness of Fraud

Group Security is responsible for promoting fraud awareness throughout the enterprise including scheduled and ad hoc activities.

The primary purpose of fraud education and training is to raise general awareness through online and face to face learning. This training will:

- Create and maintain awareness of fraud related risks
- Enable staff to identify fraud risks or red flags pertaining to fraudulent activity
- Educate staff as to how to report fraud
- Provide periodic reinforcement of fraud control principles

Employee fraud awareness training is important for the prevention and control of both internal and external fraud. Initial training is delivered to all staff through APG's induction program, embedded in the 'Better Decisions for a Better Future' e-learning module.

APG will provide regular and ongoing fraud awareness to staff which includes information and training on fraud prevention, detection and reporting. Training will be scheduled and ad hoc with opportunities for managers to schedule fraud training for their teams through Group Security (fraud@auspost.com.au).

It is the responsibility of management to promote an ethical culture and to encourage staff to speak out against fraudulent acts against APG, whether committed by staff or others.

3.6. Employment screening (pre-employment and on promotion)

In accordance with APG's employment screening and Australian Standard AS 4811-2006, People and Culture conducts pre-employment screening of all new employees and contractors joining the

Enterprise. All persons employed in positions with increased responsibilities and higher fraud risk areas will be subjected to 're-screening' as part of our risk-based approach.

APG is committed to recruiting and retaining the best employees. The recruitment process is designed to ensure that the people selected can provide quality services and uphold APG's values.

Screening information collected, with the applicant's informed consent, includes the following:

- Information on employment history and eligibility for work, including whether the applicant has previously worked for APG (including subsidiary businesses)
- Information to establish the identity of the applicant
- Character check which includes a police check must be completed before the individual receives an offer of employment and before commencing employment
- Referee comment on the applicant's conduct and behaviours in the workplace
- Medical assessments and examinations are conducted, where relevant to the role, to find out if the person can safely meet the inherent requirements of the position
- Pre-employment Services (PES) conducts a visa check on all candidates who are not citizens or permanent residents of Australia

3.7. Annual leave and job rotation

Staff holding excess annual leave can be an indicator of an area where fraudulent activity may be taking place. Business units are responsible for developing processes which ensure effective management of annual leave balances.

3.8. Supplier vetting

Those engaged in contracting to external suppliers/vendors are to take steps to ensure the credentials of new suppliers are reviewed periodically as part of due diligence. Supplier credential checks could consider:

- Searching open source locations such as the Internet for any adverse news on the supplier and the supplier's key controllers such as the company's owner/s, the CEO and/or it senior manager/s
- Consulting with other businesses or government entities who use the supplier to identify any concerns
- Evaluating any suspicious activity observed by the business during the life of the relationship, such as presentation of incomplete, incorrect or inflated invoices

APG should consider its ongoing commercial relationship with the other party if an inquiry finds a heightened risk of fraud in continuing to deal with that party. Consideration should also be given to whether new suppliers may have a conflict of interest in their engagement with the business.

4. Fraud Detection

4.1. Fraud detection system and program

APG is committed to detecting fraud within the organisation through a thorough and effective detection program. Business units will be periodically assessed to ensure there are appropriate detection capabilities in place to identify internal and external fraud.

APG has a Whistleblower program in place which includes a 24/7 confidential hotline (1800 799 353) and an email (whistleblower@auspost.com.au) that can be used to provide information anonymously and provide protection for whistleblowers under the legislation.

Group Security will liaise with Internal Audit to ensure systems or processes at risk of fraud are regularly audited.

4.2. Defining the external auditor's role in the detection of Fraud

It is the external auditor's role to provide reasonable assurance that the financial statements are free of material misstatements.

4.3. Third line auditing

Third line audits may be undertaken to examine APG's fraud control program. These audits will be conducted in accordance with the Australian Audit Standards and will incorporate the requirements of ASA 240 to consider fraud.

4.4. Managing a report of Fraud

All reports of suspected or detected fraud are to be referred to Group Security (fraud@auspost.com.au). When reports or allegations of fraud are received by the business, every effort will be made to deal with these reports confidentially, professionally and decisively.

The National Fraud and Security Risk Advisor, or nominee, will record all reports of suspected or detected fraud, noting the nature of the report, the time received and remedial actions planned and taken. Records will be kept in the Fraud Incident Register.

In examining cases of suspected or detected fraud, management and staff must ensure their inquiries do not prejudice any subsequent investigation. If in doubt, do not pursue any further investigations and contact Group Security.

Group Security will ensure all referrals are managed in a confidential manner and all cases will be treated on a need-to-know basis affording the person making the disclosure all the protections under relevant legislation and policies.

4.5. Mechanisms for reporting suspected or detected Fraud incidents

When an instance of suspected or detected fraud is identified, an initial report can be made by any member of staff, the public, third party contractors, clients, external agencies to any of the following persons:

- Immediate supervisor or manager of the staff member who is alleged to have engaged in conduct that constitutes or may constitute fraud (unless that person may be implicated)
- Any member of Group Security
- Any senior leader within the organisation
- Whistleblower hotline
- State or federal law enforcement agency

Any reports of suspected or detected fraud that are made to APG (whether to a supervisor, manager or senior leader) are to be referred to Group Security (fraud@auspost.com.au). This is irrespective of whether the matter has also been reported to the police for action.

Group Security may:

- Determine if the matter is a possible criminal offence, or a possible misconduct matter
- If the matter is determined as unlikely to be a possible criminal offence, refer the matter to a business line manager or the People and Culture team for investigation
- If the matter relates to alleged criminal conduct by an APG employee, report the matter to the Police and manage the involvement in any subsequent criminal investigation

Note: If the matter is determined not to be a criminal matter, Group Security may not manage the investigation and refer the matter through the appropriate internal channels for resolution. Misconduct investigations are managed by business line management and/or the People and Culture team. Group Security will determine their involvement based on resources and skills required. Any fraud, whether it is a protected disclosure or not, can be reported through APG's Whistleblower program for assessment.

Reports of suspected or detected fraud can be made:

In writing:

Group Security

Attention: National Fraud and Security Risk Advisor

Level 18, 111 Bourke Street, Melbourne VIC 3001

By telephone:

Whistleblower Hotline - 1800 799 353 (24hr answering machine and available internationally)

By email:

fraud@auspost.com.au or whistleblower@auspost.com.au

4.6. Obligations of reporting Fraud by a Subsidiary

As part of good governance, APG expects its Subsidiaries to ensure they have robust anti-fraud practices and procedures in place, as per the APG Group Fraud Policy.

Subsidiaries are required to notify Group Security of a suspected or detected fraud within, or concerning their business. Assistance may be provided in responding to reports of fraud, and reporting back to Group Security and to the Board Audit and Risk Committee.

4.7. Reporting suspected or detected Fraud to Law Enforcement agencies

APG requires all allegations of criminal misconduct to be reported to the relevant law enforcement body through Group Security. For all fraud related matters, Group Security must be notified as soon as possible if the matter has already been reported to the police.

4.8. Implementing a whistleblower protection program

APG's Whistleblower Program is available to current and former APG employees. The program is managed by the People and Culture team, who are responsible for handling all whistblower matters including, receiving disclosures which may be assessed as being protected and the welfare for those making a protected disclosure or complaint.

Further information in relation to APG's handling of whistleblower information can be found in the Group Whistleblower Policy and Standard.

5. Fraud Incident Response

5.1. Procedures for investigation of suspected or detected Fraud

APG will assess all instances of suspected or detected fraud and where appropriate, will take action including pursuing disciplinary action, civil legal action and/or referral to law enforcement agencies.

Group Security will assess each matter on its own merits and apply a two-stage process of investigation, endeavouring to investigate all incidents of internal fraud. External fraud will only be investigated when assistance is requested by an external agency, or where there is benefit to APG.

Stage One – Preliminary Assessment

Group Security will apply the following criteria to the incident or allegation to assess the appropriateness for further investigation:

- Determining if the referral meets the criteria of a criminal fraud offence under Part 7.3 in Chapter 7 of the Criminal Code Act (1995), or if it relates to another offence (theft, etc.)
- Determining if the suspected or detected fraud is a possible civil offence or an internal misconduct matter for referral to the People and Culture team. All referrals will be recorded in the Fraud Incident Register regardless if they progress or are recorded as 'No Further Action'
- Sufficient information to investigate

Stage Two – Investigation

The investigation will establish whether a fraud may have occurred and, if so, what action APG can take. This will be managed by Group Security in conjunction with the relevant business unit. APG conducts investigations for all reported fraud referrals in accordance with the Australian Government Investigations Standards (AGIS 2011).

For potential criminal matters, an investigation should be managed by Group Security to ensure the investigation is conducted in a manner consistent with a criminal investigation process, can apply measures to make sure all evidence is collected in an admissible manner, and that procedures are followed to ensure any subsequent law enforcement investigation is not compromised. Investigations will be conducted in a manner that affords all parties their basic human rights and natural justice.

The objective of an investigation in this context is to:

- Identify evidence that is material in determining an allegation of improper conduct
- Establish the identity of the alleged person(s) engaging in improper conduct
- Establish a nexus between the individual(s) and the alleged conduct

It is also important when conducting or managing an investigation to:

- Gather relevant information in a timely and legally admissible manner
- Protect the privacy of those making an allegation and other witnesses

Group Security is authorised under the Australian Postal Corporations Act 1989 *'for ensuring the integrity of the functions of Australia Post. Investigators are authorised to enter postal facilities and other premises used for the conduct of the business of the Corporation, to interview employees and members of the public on official business, to examine official records and to take possession of Corporation property for inspection or evidentiary purposes'*.

When necessary, and as part of the investigation process, Group Security will enlist the assistance of external agencies. All matters that may lead to law enforcement referral or disciplinary action

must be investigated by an appropriately skilled and experienced investigator appointed by Group Security. All investigations involving criminality or potential criminality will be subject to an appropriate level of supervision by Group Security.

Investigation of improper conduct may involve the following core activities:

- Interviewing relevant witnesses including obtaining statements where appropriate from witnesses internal and external to the business
- Reviewing and collating documentary evidence
- Forensic examination of computer systems
- Forensic accounting
- Examination of telephone records and APG issued mobile devices
- Enquiries with banks and other financial institutions (subject to being able to obtain appropriate court orders if necessary)
- Enquiries with other third parties
- Data search and seizure
- Data analytics
- Expert witness and specialist testimony
- Tracing funds/assets/goods
- Preparing briefs of evidence
- Liaison with the police or other law enforcement or regulatory agencies
- Report preparation

5.2. Internal reporting and escalation

It is the responsibility of Group Security to escalate any major fraud matters within APG. All employees must notify Group Security of any fraud that they are aware of for inclusion in internal reporting. Matters involving material loss, media attention, potential political notice, or potential for criminal charges against a staff member should be reported immediately.

Reporting consists of the preparation of material for internal consumption and includes Board Audit and Risk Committee and (external) government reporting.

5.3. Fraud Incident Register

In line with the Australian Standard AS/NZ 8001-2008 Fraud and Corruption Control, the APG Fraud Incident Register includes:

- Date and time of report
- Date and time of incident detection
- Where the incident took place (e.g. Procurement)
- How the incident was reported
- Nature of the incident
- Value of the loss to APG (or external party)
- Action taken

5.4. Disciplinary procedures

All possible outcomes for resolution are considered in alignment with the People and Culture team's disciplinary or dismissal procedures. Action will be aligned to:

- Our Ethics
- Group Fraud Policy

If during a disciplinary investigation it is determined that criminal offences may have been committed, a referral may be made to law enforcement. APG may still follow through with disciplinary action regardless of the outcome of any criminal prosecution.

Persons covered by the policy, who are terminated as the result of alleged fraudulent conduct, will be registered as those not eligible for further engagement with APG.

5.5. Policy for civil proceedings to recover the proceeds of fraud

If legal proceedings are to be considered to recover funds or value of assets lost due to fraud or misappropriation, Group Legal should be contacted for advice.

Avenues may exist for APG to take immediate civil recovery procedures, or through the criminal court system by way of an application for restitution upon sentencing of a convicted individual.

Where there is clear evidence of fraud and, where the likely benefits of such recovery will exceed the funds and resources invested in the recovery action, then recovery action will be undertaken.

5.6. Internal control review following discovery of Fraud

To ensure control weaknesses are rectified, a review of the internal control environment should be performed by the relevant business unit, in consultation with Group Risk and/or Internal Audit, after an incident of fraud has occurred.

In cases of material fraud, Internal Audit may conduct an internal control review to evaluate the effectiveness of the controls in preventing further such incidences. Review outcomes may include the need for new or strengthened controls, revised policy or procedure, additional staff training and increased frequency of Internal Audit reviews.

5.7. Insurance

For information about the adequacy of APG's insurance in relation to fraud or improper conduct, contact the Manager - Insurance, Risk and Compliance (insurance.notification@auspost.com.au).

Group Security will notify the Manager - Insurance, Risk and Compliance of suspected material fraud as soon as possible after the allegation is received.

Glossary

Term	Definition
APG	Australia Post Group (APG) is defined as the Australian Postal Corporation and its subsidiaries.
Fraud	Any intentional act by one or more individuals (internal and external), involving the use of deception or misrepresentation to obtain an unlawful advantage to the detriment of the Australia Post Group.
APG Staff	APG Staff is defined as anyone who performs services for the Australia Post Group, or on its behalf, and includes: • employees of any company in the Australia Post Group • contractors, consultants, licensees and agents (and their employees and subcontractors), who perform services for the Australia Post Group • any other third parties performing services for or on behalf of the Australia Post Group
Whistleblower Policy and Standard	The APG policy and procedure for receiving, handling and investigating any suspected wrongdoing or problems which, by their nature or circumstance, cannot be raised through the standard reporting line. Whistleblower disclosures can be reported to an independent, external agency.

Document Control

Document Information	
Document Title	Enterprise Fraud Framework
Version No	1.0

Framework Owners and Governance Forums

Owner / Forum	
Accountable Executive	Chief Risk Officer
Framework Owner	Head of Security Operations
Framework Administrator & Content Owner	National Fraud and Security Risk Advisor

Key Dates

Administrative Area	Date
Framework Approval Date	10 March 2020
Framework Effective Date	10 March 2020
Next scheduled review	2021