Challenger Limited

Fraud and Corruption Policy

This version:	Version 7.6
Jurisdiction:	All
Date of version:	May 2022
Review of policy due by:	November 2023
Policy owners:	Head of Financial Crime, Group & Corporate Risk
Prepared by:	Risk and Compliance
Authorised by:	Group Risk Committee

challenger

SUMMARY

Why is this policy required?

The purpose of this policy is to proactively minimise Challenger Limited and its subsidiaries' ('Challenger') exposure to fraud and corruption, including dishonest acts, bribery, misuse of position, malicious and reckless behaviour and criminal acts committed by employees, contractors, clients or third parties. It has been developed to create consistency across all divisions of the Group.

To whom does this policy apply?

This policy applies to all employees of the Group, regardless of division and the consultants, directors, officers, agents and contractors who directly or indirectly, provide services to, or act for or on behalf of Challenger from time to time (who are collectively referred to as 'employees' throughout this policy).

Reporting Requirements

Cases of suspected / actual fraud and/or corruption are to be reported in accordance with the procedures outlined in this policy.

Risk and Compliance provide reporting to the Group Risk Committee (GRC) and subsidiary Risk Committees in relation to fraud risk management and fraud incidents.

Training and Awareness

Employees are provided with information regarding this policy upon commencement. The policy is available via the company intranet site (Connect). Targeted training sessions in relation to specific elements of this policy are delivered from time to time.

Key Terms

Fraud	*Dishonestly obtaining a benefit, or causing a detriment to another, by deception or other means.*
Corruption	*Dishonest or fraudulent conduct by those in power, typically involving bribery.*
Bribery	*To promise or provide undue benefit to another person with the intention to influence the winning or retention of business, or any other benefit.*
Facilitation Payment	*A payment of a minor value made for the purpose of expediting or securing the performance of a routine government or official action. The payment cannot determine the action.*

Review Cycle

This policy will be reviewed and updated as required due to business and external considerations and at least every two years.

The supporting procedures to this policy (not published with this policy on the Challenger Public Website) will be updated and amended on a periodic basis or as deemed necessary by the Head of Financial Crime, Group and Corporate Risk.

1. Why does Challenger need a Fraud and Corruption Policy?

Challenger is committed to the highest level of integrity and ethical standards in all business practices. It is our policy to conduct all of our business in an honest and ethical manner. Challenger recognises that the management of fraud and corruption is integral to good governance and management practice, and accordingly has implemented a robust Fraud and Corruption Framework.

The purpose of this policy is to proactively minimise Challenger's exposure to fraud and corruption, including dishonest acts, bribery, misuse of position, malicious and reckless behaviour and criminal acts committed by employees, contractors, clients or third parties. It has been developed to create consistency across all divisions of the Group. Specific objectives of this policy include:

- Protect Challenger's assets and reputation;
- To confirm the organisation's commitment to a sound ethical culture and risk management system;
- Ensure senior management commitment to identifying risk exposures to fraud and corrupt behaviour and for establishing procedures for prevention and detection;
- Monitor and review fraud and corruption controls on an ongoing basis; and
- Ensure employees are aware of their responsibilities in relation to ethical conduct.

2. What is fraud and corruption?

2.1 Fraud

Fraud can occur in a variety of ways and it is important for everyone at Challenger to have a good understanding of what constitutes fraud so that they can recognise it and take action to prevent it.

For the purpose of this Policy, fraud is defined as:

> ***'Dishonestly obtaining a benefit, or causing a detriment to another, by deception or other means'***

Note that while conduct must be dishonest for it to meet the definition of 'fraud', the conduct may not necessarily constitute a breach of the criminal law.

Fraud includes:

- Obtaining property, a financial advantage or any other benefit by deception
- Theft of physical, financial or intellectual assets (including customer data)
- Causing a loss, or avoiding or creating a liability by deception
- Providing false or misleading information to Challenger, or failing to provide information where there is an obligation to do so
- Making, using or possessing forged or falsified documents
- Unauthorised internal or external access to, or interference with, a Challenger IT system
- Charging Challenger for goods or services that are incomplete, not delivered or inconsistent with Challenger's Expenditure Policies and Guidelines.
- Acting on conflicts of interest to gain personal advantage (at the detriment of Challenger or its customers)
- Any offences of a like nature to those listed above.

2.2 Corruption

For the purpose of this policy, corruption is defined as:

> ***'Dishonest or fraudulent conduct by those in power, typically involving bribery'***

This includes:

- Public officials misusing position and/or powers for personal / related party gain
- Persons in private positions of power misusing this for personal / related party gain
- Improper business arrangements

- Third party demanding lavish entertainment or gifts before commencing or continuing negotiations
- Accepting lavish gifts or entertainment in exchange for business favour
- Third party demanding payments to overlook our competitors' proposals
- Third party requests that we provide employment or some other advantage to a friend or relative
- Third party demanding payment in order to 'overlook' potential legal or other violations
- Paying or receipt of bribes (payments aimed at influencing the outcome of a transaction)
- Making 'facilitation payments' to expedite the performance of government-controlled processes
- Paying secret commissions to those acting in an agency or fiduciary capacity

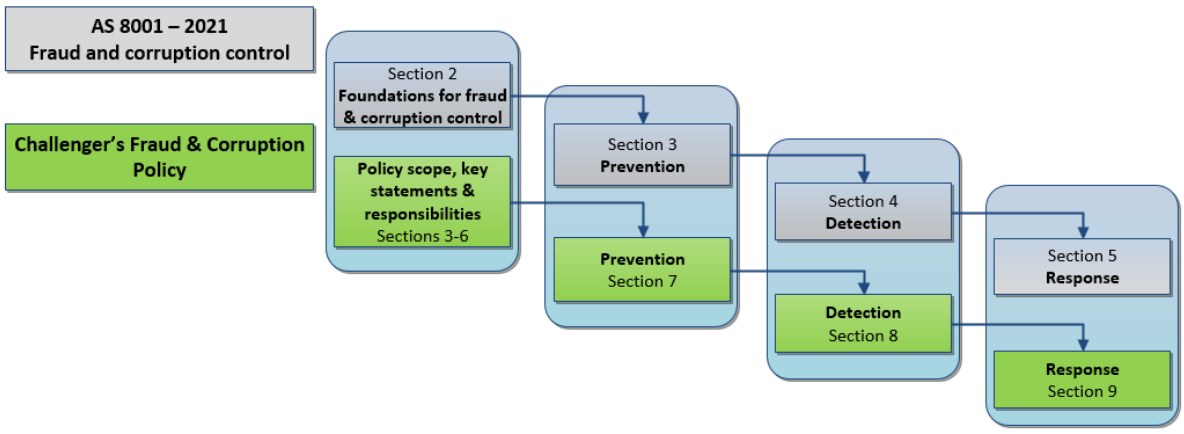
3. Challenger's policy on fraud and corruption

3.1 Overview

Challenger is committed to ensuring a corporate culture of honesty and integrity in which employees understand that fraud and corruption will be detected and responded to. Challenger does not apply any materiality threshold for internal fraud and corruption. Internal fraud and corruption will not be tolerated in any form.

All employees are accountable for, and have a role to play in, fraud and corruption control. Employees have a duty to familiarise themselves with the operating procedures, controls and delegations of authority applicable to the responsibilities of their role and to be alert for any indications of irregularity. Employees are encouraged to report suspected fraudulent or corrupt activities per the procedures outlined in this policy. Suspected fraudulent or corrupt activities will be thoroughly investigated and responded to appropriately. Challenger will also protect the anonymity of anyone reporting suspect activities.

This policy has been developed and structured with reference to the Australian Standard on Fraud and Corruption Control AS8001-2021 and key elements of the Anti-Bribery Management System ISO standard (ISO37001:2016) have been considered.



3.2 Position on facilitation payments and approach to gifts, benefits and entertainment

Facilitation payments are payments of minor value for the purpose of expediting or securing the performance of a routine government or official action. Should the payment also "determine" the outcome of the action it could no longer be considered as a facilitation payment, this would constitute a bribe.

As there is a risk that facilitation payments could be interpreted as bribes, they are prohibited by Challenger. In no circumstances may Challenger or its employees make facilitation payments when dealing with government bodies in Australia or overseas.

It is not the intention of this policy to prohibit normal and appropriate hospitality (given or received in accordance with company policies and the law generally) to or from third parties. However, it is essential to avoid the possibility that the gift, entertainment or other business courtesy could constitute or be perceived as a bribe. Challenger's Gifts, Benefits and Entertainment Policy sets out clear protocols for employees around the giving and receiving of gifts and other benefits, and how these must be reported and approved. The Risk and Compliance function performs periodic assurance reviews of employees' compliance with the policy, with results reported to the GRC.

3.3 Position on political donations

Challenger has adopted a policy of not making political donations in any country or jurisdiction in which it operates. The policy prohibits entities within the Challenger Group from making donations, or contributing funds, to any political party, parliamentarian, elected official or candidate for political office and prohibits Challenger employees, executives and directors from attending events, in their official capacity, where funds are raised for these purposes ('political fundraising events').

4. Applicability

This policy applies to all employees of Challenger, regardless of division and the consultants, directors, officers, agents and contractors who directly or indirectly, provide services to, or act for or on behalf of Challenger from time to time (who are collectively referred to as 'employees' throughout this policy).

Entities and Divisions that have operations in jurisdictions other than Australia must consider local rules and regulations that may require stricter practices than those set out in this Policy. Where local rules are more stringent than those outlined in this policy, the local regulations will always prevail. If there is a direct conflict between local laws and the requirements under this policy, the Policy Owner must be notified prior to implementing local policies or procedures.

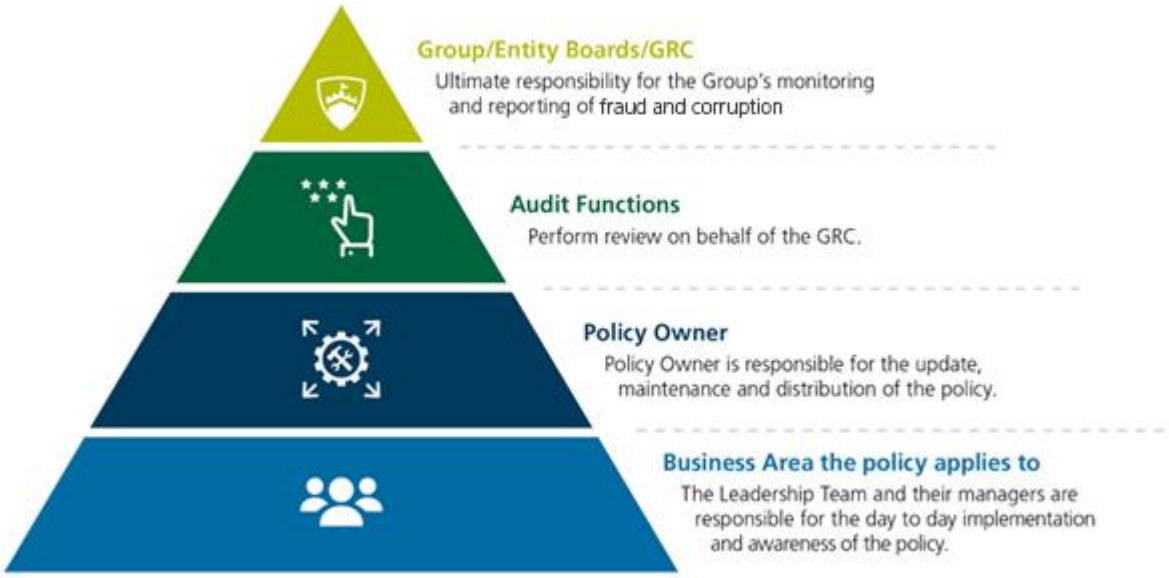
5. References

This policy should be read with reference to the obligations laid out in Challenger's policies, practice notes and other documentation as amended from time to time, including but not limited to:

- Code of Conduct
- Challenger Values
- Conduct Risk and Consequence Management Framework (CRCM Framework)
- Financial Abuse of Elders and Vulnerable Customers Framework
- Challenger Risk Appetite Statement
- Operational Risk Policy and Operational Risk Practice Note
- Challenger AML/CTF Program and Policy
- MLMF (the Bank) AML/CTF Program
- Incident Management Policy
- Whistleblower Policy
- Employee Due Diligence Policy
- Transaction execution sign-off processes
- Gifts, Benefits and Entertainment Policy
- Political Donations Policy
- Expense Policies and Guidelines
- Outsourcing Policy
- IT Security Policy
- Internal Privacy Policy

6. Overall Responsibilities

Fraud and corruption prevention and detection is the responsibility of all Challenger employees. However, the following specific responsibilities apply:



The Group / Entity Boards and Directors bear the ultimate responsibility for corporate governance, fraud and corruption prevention and management. The GRC has been established to assist them in discharging these responsibilities.

The GRC has oversight responsibility for fraud and corruption management across the Group. The GRC will receive reporting relating to the implementation of the policy and any matters reported to the Chief Risk Officer (CRO) under this policy.

Any suspected cases or incidents of fraud concerning the Chief Executive Officer will be reported to the Chair of the GRC who will determine the appropriate mechanism to promptly investigate the incident.

The Bank Risk Committee (BRC) for MLMF (the Bank) will receive regular reporting from the Bank CRO or delegate relating to KRIs for financial crime, as identified within the Bank. Relevant reporting will be provided through to the ERMC and GRC.

Internal audit performs targeted reviews on behalf of the GRC on fraud and corruption governance, procedures and implementation effectiveness. Aspects of the overall effectiveness of the fraud and corruption framework may also be covered in the External Audit cycle and recommendations included in their audit reports, as well as through periodic monitoring reviews undertaken by the Risk and Compliance team under Challenger's Line 2 Assurance Program. As Policy Owner, the Head of Financial Crime, Group and Corporate Risk (Head of FCR) within the Risk and Compliance Team is responsible for ensuring the policy is kept up to date, maintained and distributed to the business.

The Leadership Team (Chief Executives) and their managers are responsible for fraud prevention and detection management. This includes:

- Identification of new and emerging fraud and corruption risks
- Adopting preventative measures to deter and detect instances of fraud and corruption
- Reporting all instances of suspected or actual fraud and / or corruption in accordance with the escalation procedures outlined in this policy.
- Exercising due diligence and control to prevent, detect and report acts of fraud and / or corruption
- Setting an example and advising employees of the acceptability or otherwise of their conduct.
- Ongoing management of risks and control activities.

Employees are responsible for reporting all instances of suspected fraud and/or corruption.

7. Prevention

7.1 Integrity framework

Challenger is committed to meeting high ethical and consistent professional standards in the way it conducts its business. This commitment is evident throughout Challenger's Risk Appetite Statement. Challenger has also developed and communicated to employees a Corporate Code of Conduct ('the Code') and a set of work-related behaviour values for employees which includes 'Act with integrity'.

Challenger's recruitment process requires that all new employees read and acknowledge that they understand and will abide by the requirements of the Code. The Code requires employees to adhere to Challenger's policies. Behaviour of a kind that involved an act of fraud and / or corruption would breach at a minimum the requirement to 'act honestly and display a high level of integrity'. Failure to comply with the Code may result in Challenger taking disciplinary action against the individual up to and including termination of employment.

One of the techniques used to monitor the health of Challenger's culture is the monitoring of adherence to the Challenger Values as part of the annual employee performance review process. The values articulate clear behaviour expectations for employees. Employees falling short of meeting the behaviour standards as assessed against the values, will not be eligible to participate in any Employee Incentive Program.

7.2 Senior management commitment to controlling the risk of fraud and corruption

Board reporting from the Group CRO includes summaries of Operational Risk (including fraud / corruption) incidents and Financial Crime Risk activities. This provides ongoing awareness at the most senior level of the organisation of the level of fraud and corruption observed by the organisation both internally and externally.

In addition to this, management are engaged in operational risk coverage reviews (covering all operational risks including fraud and corruption) run on a periodic basis to confirm existing and identify emerging risks.

7.3 Line management accountability for controlling fraud and corruption

Managers are expected to be aware of and display behaviour consistent with the company Code of Conduct. Management undertake performance assessments of their employees on at least an annual basis. Managers are responsible for taking action in relation to behaviour inconsistent with the Code or Challenger Values.

Where material fraud and corruption risks are identified in the Operational Risk Framework, risk ownership is established and the risk owner is responsible for the development of mitigating controls, including assignment of accountability for each control. The Operational Risk Policy and Practice Note details the processes and procedures undertaken.

7.4 Maintaining an internal control system and culture

All material fraud and corruption risks identified within the Risk Framework have control sets framed around the risks with specific accountabilities established.

A number of key controls have also been implemented through the Challenger and MLMF AML/CTF Programs focused on the identification of customers, customer transactional patterns and the employee recruitment process. These AML/CTF Programs provide further detail.

Key controls are captured within the governance, risk and compliance system and assessed through periodic risk and control self-assessments as well as compliance attestations to the operational effectiveness of controls. This systematic approach to the identification, documentation and monitoring of controls provides ongoing reinforcement of the control culture. Internal Audit undertake targeted reviews on behalf of the GRC on operational governance, procedures and control effectiveness in line with the Internal Audit Plan. Control weaknesses identified, (including controls relevant to fraud and corruption) are reported through to the GRC with audit points raised to be addressed by management. Challenger's Information Security Management System (ISMS) is outlined in the Information Security Policy, which is aligned to ISO/IEC27000 and NIST framework. Challenger understands the increasing threat to organisations (and their critical data assets) posed by

cyber-enabled fraud and has appointed a Chief Information Security Officer (CISO) who is accountable for the design and overall implementation of the policy. The CISO collaborates closely with the Risk and Compliance team to ensure IT security risks are managed in accordance with Challenger's operational risk management framework. This includes ongoing engagement with the Head of Financial Crime, Group & Corporate Risk (Head of FCR) to ensure information security incidents with a potential fraud and/or privacy impact are assessed and reported in accordance with internal procedures and external reporting obligations.

7.5 Fraud and corruption risk assessment

Fraud and corruption risks are identified, rated and regularly assessed as part of the overall Group Risk Management process. This process includes activities to regularly (typically every 18 months to two years or on substantial business change) assess the risk profile of the business including the capture of emerging fraud and corruption risks. This process will involve consideration of internal risk drivers (e.g. business change or fraud events) or external risk drivers (e.g. external environment scanning to identify vulnerabilities and threats at an industry level). The identification of new fraud and corruption risks may also occur through undertaking a Delivered Risk Assessment prior to implementing a specific business initiative. From time-to-time targeted assessments may be undertaken on specific risk exposures, for example, an assessment may be targeted on bribery and corruption.

Operational deep dives / scenario analysis is also an integral component of the Operational Risk Management Framework. At least one fraud or corruption scenario analysis is undertaken approximately every 2 years. The scenario will be determined by the Risk and Compliance Team.

7.6 Communication and awareness of fraud and corruption

Challenger provides employee training and utilises existing communication mediums to increase awareness. Challenger raises awareness of the Code and this policy to ensure employees are aware of their responsibilities and role in combating fraud.

Key processes and communication channels are leveraged in order to provide employees with an awareness of what constitutes fraud and corruption and Challenger's zero tolerance position in relation to internal fraud and corruption.

Specific activities include:

- This policy is available to all employees on the Challenger intranet.
- On employment all new employees are asked to sign that they understand and will abide by the Challenger Code of Conduct.
- On commencement and then periodically in accordance with Challenger's online learning program, all employees must complete the Risk and Compliance Computer Based Training Model, which addresses matters relating to fraud and conflicts of interest management.
- On at least an annual basis employee performance is assessed and measured against the Challenger Values. The 'Act with Integrity' value supporting behaviours include considering and planning for current and future risks, acting honestly, respecting and abiding by our regulatory obligations and speaking up when things are not right.
- Management, who are best placed to manage and mitigate material fraud and corruption / bribery risks identified in the operational risk register, design and maintain the treatment / control sets and assess their effectiveness on a periodic basis.
- All employees in roles associated with increased financial crime-related risk are required to complete the AML/CTF Computer Based Training module. They must reconfirm their competency by passing an AML/CTF knowledge assessment periodically.
- Front line / customer facing employees have been trained on the existing customer identification requirements and also scenarios that might constitute suspicious behaviour as part of the relevant AML/CTF Program.
- Targeted teams who are more likely to encounter fraud and / or corruption in their roles are provided specific fraud and corruption awareness training (typically face-to-face). Targeted training may also be conducted for particular teams following a fraud-related incident or 'near-miss' event.
- Ad-hoc workshops are undertaken with employees.
- 'Pressure-testing' may be employed to test the operational effectiveness of key controls through submission of test transactions (for example, false invoices or bank change requests)

- Targeted ‘phishing campaigns’ for employee groups, and ‘Red-teaming’ exercises to identify IT security vulnerabilities as part of the ISMS

7.7 Employment screening (pre-employment and on promotion or transfer)

Challenger conducts pre-employment screening for new permanent employees and contractors on a term of greater than 3 months. Where practical these checks are undertaken prior to commencement of employment. In all other circumstances, the continuance of the employment contract is contingent on the satisfactory outcome of the remaining probity checks. The Challenger Employee Due Diligence Policy provides further detail.

7.8 Policy dealing with taking annual leave

Challenger encourages all employees to take their full leave entitlement each year. It is mandatory for all employees that at least two weeks of this leave is taken on a continual basis (inclusion of one day statutory holiday over the two weeks is acceptable). Completion rates are tracked via the Human Resources System, analysed and communicated through to Management and Business Heads as necessary.

7.9 Customer, supplier and other counterparty due diligence

In order to reduce fraud and corruption exposures due diligence is applied to third parties and is intended to establish three key points:

1. Verify the identity of the third party
2. Establish whether the third party has any higher risk attributes such as criminal history or close links to political persons
3. Confirm that the third party is not listed on an Australian or other relevant sanctions list.

Specific due diligence required:

Customers

On the provision of the majority of the designated services defined under the AML/CTF Act, Challenger is required to undertake customer identification and verification processes to confirm the identity of the customer. Challenger also checks its customers against watch-lists to identify potential sanctioned parties and also any potential Politically Exposed Persons. Further verification may also be required as part of the ongoing customer due diligence process on any existing customer. Some designated services, for example securities traded on recognised exchanges may be exempt from these requirements.

Suppliers

All new Australian domestic supplier’s ABN numbers are checked on the ABR government website before they are set up on the Accounts Payable system. Company registration and name are verified and this also assists with GST requirements.

Associated material invoices are automatically matched against purchase orders in the Accounts Payable system with all invoices also approved in line with the authorities as delegated within this system.

In regard to non-Australian domestic operations as the current supply base is more consolidated and any specific due diligence is undertaken as determined necessary by local management.

Challenger has an Outsourcing Policy which provides supplier due diligence guidance for employees when contemplating an outsourcing arrangement. Please see the Outsourcing Policy for further detail.

Other Counterparties

Other counterparties would include organisations and/or individuals who Challenger either directly buys or sells assets or securities to/ from or those who assist Challenger in the execution of such transactions. Where designated services per the AML/CTF Act are not provided the default due diligence position in regard to establishing the identity of the entity or individual is to an equivalent standard to the Australian AML/CTF checks and to include watch-list screening.

In recognition that this default position may not be appropriate in all cases, a list of standing exemptions to the identification and watch-list screening due diligence process is also provided in

supporting procedures to this Policy. From time to time exemptions (identification, watch-list screening or both) outside of this standard list may be appropriate and these may be granted by the relevant Chief Executive or delegate in conjunction with the Head of FCR (in countries considered as lower risk per Challenger's risk rating methodology). Where the counterparties are based outside of these lower risk jurisdictions, the CRO must also support the exemption. All other exemptions (i.e. that are not standing exemptions), need to be documented with full rational articulated in transaction documentation.

Identity verification issues and potential watch-list matches

Should the identity of a customer, supplier or other counterparty be difficult to establish the matter should be referred to the Financial Crime Risk team for assistance. All potential and positive watch-list matches need to be referred to the Financial Crime Risk team for confirmation and will be referred to the relevant Chief Executive should they be considered to present any significant business / transaction risk.

8. Detection

8.1 Fraud and corruption detection program

Due to the multifaceted nature of fraud and corruption combined with the relatively modest scale of the Challenger business the organisation is reliant on employees and management awareness of the need to, and integrity in, escalating and reporting suspicious activity.

Some additional tools have also been developed, primarily leveraging AML/CTF legislative requirements, that set the minimum identification and verification requirements for new customers and also monitor transactions for suspicious activity.

8.2 Red flags and warning signs

8.2.1 Red flags and warning signs for internal fraud

In many situations where internal fraud has emerged the individuals either working alongside the perpetrator/s or with the information provided by them have experienced growing levels of discomfort that things did not seem to be quite right.

Having management and employees recognise and report these suspicious situations is an important component for the effective detection of fraud.

The following list provides examples of the red flags and warning signs of internal fraud:

1. Behavioural – objective

- Changes to working patterns, long hours after normal business hours
- Long absences from work, poor timekeeping, refusal to take leave
- Frequent over-riding of internal controls
- Regular and unwarranted visits to departments involved in control functions
- Unrealistic performance / profitability 'too good to be true'
- Abrupt / unexpected resignation

2. Behavioural – subjective

- Indications of change in wealth, either excessive spending or signs of financial hardship
- Reluctance / refusal to relinquish duties from a previous job function
- Evasive, ambiguous or misleading responses to questions
- Over eager to assume another's duties
- Unusually inquisitive about payment, purchasing systems and processes
- Aggressive or abusive behaviour

3. Technology systems

- Sign-ons at unusual times of the day
- Continuing to complete certain tasks remotely when away on leave
- Excessive instances of failed log-ins

In Operations teams, indicators of internal fraud may be identified through key processes like quality checking reviews and complaints management. These activities may alert Challenger to unusual activity that requires further investigation (for example, where transactions or account changes appear to have been processed without customer authorisation).

Should any Challenger employee become aware of any of these red flags / warning signs (particularly if a combination is present) without plausible reasoning, they should be reported via one of the mechanisms provided in this policy. While not designed for reporting fraud and corruption, Challenger's Exit Interview Program is another process by which indicators of potential misconduct may be identified.

8.2.2 Red flags and warning signs for customer / external fraud and corruption

The AML/CTF Act (2006) and associated rules impose minimum Know Your Customer standards and also monitoring requirements in relation to customer transaction activity. Indicators of money laundering are very similar to more generalised financial crime and Challenger has constructed its monitoring systems to detect any of the higher risk areas of financial crime. Models and related scenarios are covered in more detail in the Customer Identification Processes and the Transaction Monitoring scenarios applied in the Challenger and MLMF AML/CTF Programs.

Indicators of external fraud and corruption are documented and maintained by Challenger for internal use and reference.

8.2.3 Investment System Flags

Significant investment has also been undertaken in the asset registry and payment systems across investment portfolios. These systems provide transparency and assurance that trading activities are being undertaken within prescribed boundaries.

8.3 External audit's role

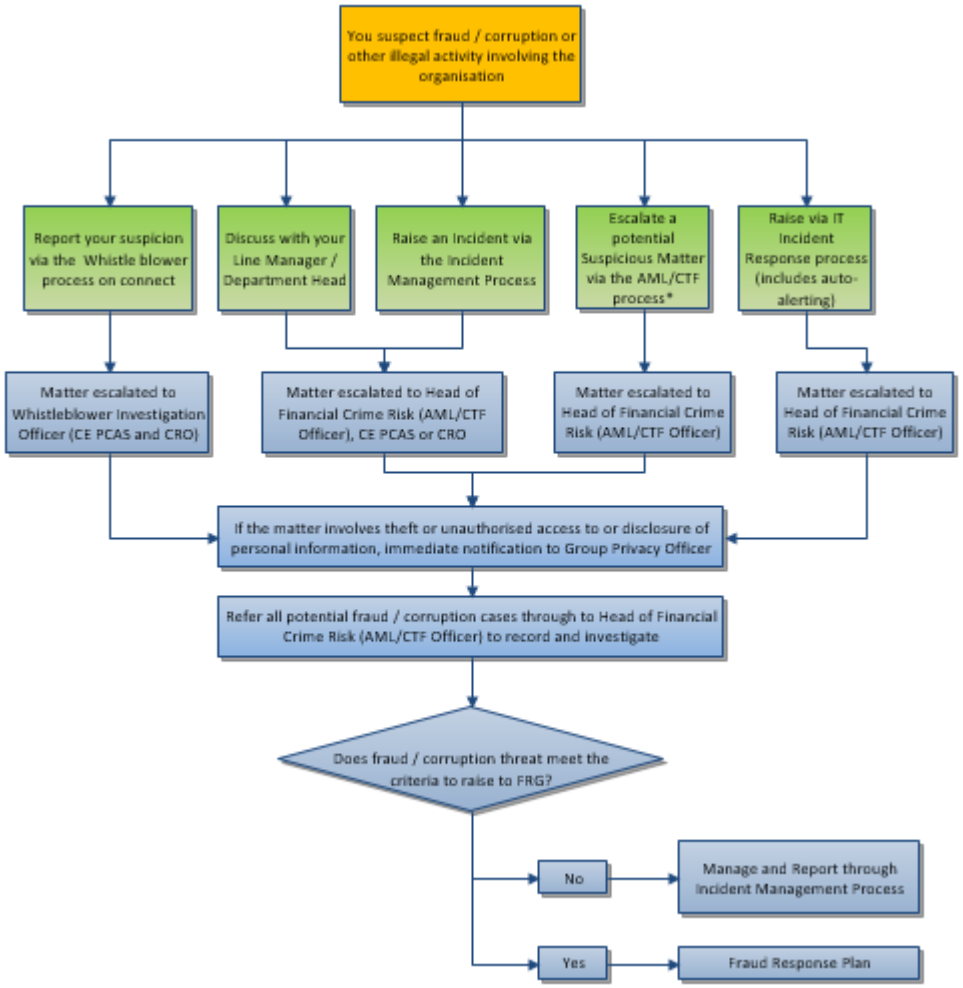
External Audit is engaged to provide an opinion on annual financial accounts. In doing so they may not necessarily identify whenever frauds or illegal acts exist, however any material abnormalities that are identified will be referred directly through to senior management, the GRC and Board. External audit also receives periodic reporting on any fraud-related incidents that have been identified for the relevant period.

8.4 Mechanism for reporting suspected fraud and corruption incidents

Challenger provides a variety of channels through which to report suspected fraud or corruption. It is mandatory for any individual suspecting fraudulent or corrupt activity to report it through at least one of these channels:

- Discuss with Line Manager or a Leadership Team member
- Raise an Incident via BRiskWise (Incident Management Process)
- Escalate a potentially suspicious matter via the AML/CTF process
- Report a suspicion through the Whistleblower mechanism
- Raise an incident via IT Incident Response Process

The following diagram illustrates the primary mechanisms for reporting suspected fraud and corruption incidents and the process for recording such incidents. It is to be followed wherever practical unless local procedures have been established as an alternate. Where local procedures do exist, it is also at the discretion of local management whether and when the Fraud Response Plan should be triggered.



*In accordance with process under the applicable AML/CTF Program

8.4.1 Whistleblower Policy

Challenger has a Whistleblower Policy and encourages disclosures from employees, former employees and suppliers regarding any unethical, illegal, corrupt or other inappropriate conduct including in relation to this policy. The Whistleblower Policy is available on Connect and www.challenger.com.au.

9. Response

9.1 Fraud and Corruption Response Plan

The Fraud and Corruption Response Plan outlines the arrangements that are in place for dealing with a detected or suspected case of fraud and/or corruption. It is intended to provide procedures which allow for evidence gathering and collation in a manner which will facilitate informed decision making, while ensuring that the evidence gathered will be admissible in the event of further civil or criminal proceedings. These procedures have been established to enable Challenger to restrict damage and minimise losses arising from fraud incidents and retain market confidence.

Where local procedures exist, it is at the discretion of local management whether to follow the Fraud and Corruption Response Plan set out below, use it as a guideline, or alternatively apply their own documented procedure.

9.2 Activation of the Fraud and Corruption Response Plan

This plan has been constructed to cover both material external frauds that could have an impact on the organisation along with all examples of corruption and internal fraud. Lesser impact external fraud

incidents will be covered within existing internal business processes. As a general guideline this plan will be enacted when:

- External fraud – any detected or suspected fraudulent activity that would be rated as a 'high' impact incident under the Incident Management Policy and Practice Note and
- Internal fraud and corruption incidents – any detected or substantive allegation of internal fraud and corruption within the organisation regardless of materiality.

The plan may be activated by any of the following; Group CRO, Chief Executive People, Corporate Affairs and Sustainability, GM Operational Risk and Compliance, Head of FCR, or Local Business Head in a non-Australian jurisdiction.

Where the fraud incident also constitutes a trigger event under the Crisis Management Plan (CMP), the Crisis Management Team (CMT) will be notified and the CMP invoked as applicable. Relevant steps set-out under the Fraud and Corruption Response Plan may be leveraged as part of the CMP.

9.3 Roles and Responsibilities in Fraud and Corruption Response Plan

The following individuals will form the basis of the Fraud Response Group (FRG). On a case by case basis and at the discretion of the Group CRO additional parties may be included (or at least provided with investigation updates, as appropriate). Depending on the circumstances and nature of potential impacts to the organisation, these parties could include the CFO, Chief Executive or CRO of the relevant business.

Group CRO

Overall accountability for the investigation of fraud and the associated actions taken for all potential / suspected fraud as defined in the scope of this response plan. Where appropriate / necessary, the Group CRO is responsible for informing internal parties and internal / external audit about the investigations. The Group CRO will inform and consult with the Group and/or Business line Chief Executives in cases where the loss is potentially significant. Where the incident may lead to adverse publicity, the Chief Executive People, Corporate Affairs and Sustainability is responsible for briefing media and investor relations personnel.

While the Group CRO will retain overall accountability, responsibility for leading any investigation will be delegated to the Head of FCR.

Significant matters will be reported to the Group and Relevant Entity's board as soon as practical.

Chief Executive (CE), People, Corporate Affairs and Sustainability

The CE, People, Corporate Affairs and Sustainability will advise the Group CRO along with those involved in the investigation in matters of employment law, company policy and other procedural matters (such as the application of consequence management procedures under Challenger's CRCM Framework or complaints procedures) as necessary.

The CE, People, Corporate Affairs and Sustainability (or appointed delegate) participates in any interviews relating to the suspected fraud where the interviewee is a Challenger employee, and will oversee any disciplinary processes in accordance with the CRCM Framework, should they be required.

General Counsel

The General Counsel will advise the Group CRO along with those involved in the investigation in matters of relevant legal constructs and considerations. This advice may be provided in relation to any investigative or recovery actions. They will also be responsible for the appropriate notification of any material matters to Challenger's insurance providers.

GM, Operational Risk and Compliance

The General Manager, Operational Risk and Compliance will advise the Group CRO in matters on regulatory and disclosure obligations along with providing support to those involved directly in the investigation and is responsible for all communications with regulatory agencies other than AUSTRAC.

Chief Information Security Officer (CISO)

The Head of Information Security will advise on matters pertaining to compromise, illicit use, attack, defacement, or infiltration of the Group's computer systems, networks, and internet facing resources.

Where required, they will engage and liaise with external cyber incident response and forensics providers, or cybercrime-specific government agencies engaged to assist in the investigation and resolution any such incidents. They will also act as a liaison with any internal IT functions as required for the purpose of clarification or investigation of any incident falling under this policy.

Head of Financial Crime, Group and Corporate Risk (Head of FCR)

The responsibility for leading any investigation will be delegated to the Head of FCR and will include;

- initiating a diary of events to record the progress of the investigation throughout
- working as a member of and in close consultation with the Fraud Response Group
- leading the initial investigation phase to validate the substance of any allegations made
- agreeing the objectives, scope and timescale of the investigation and resources required with the Fraud Response Group at the outset of the investigation;
- leading / coordinating external support in more substantial investigation exercises
- ensuring that proper records of each investigation are kept from the outset, including accurate notes of when, where and from whom evidence was obtained and by whom.
- liaising with local authorities / law enforcement as necessary

The Financial Crime Risk (FCR) team maintains a record of all reported instances of fraud, including those dismissed as minor or otherwise not investigated. Records will contain details of actions taken and conclusions reached. Updates on matters handled by the Fraud Response Group will be provided to GRC as appropriate.

In conjunction with reporting obligations under AML/CTF legislation the Head FCR is accountable for relevant information to be reported to AUSTRAC and the relevant policing authority as required.

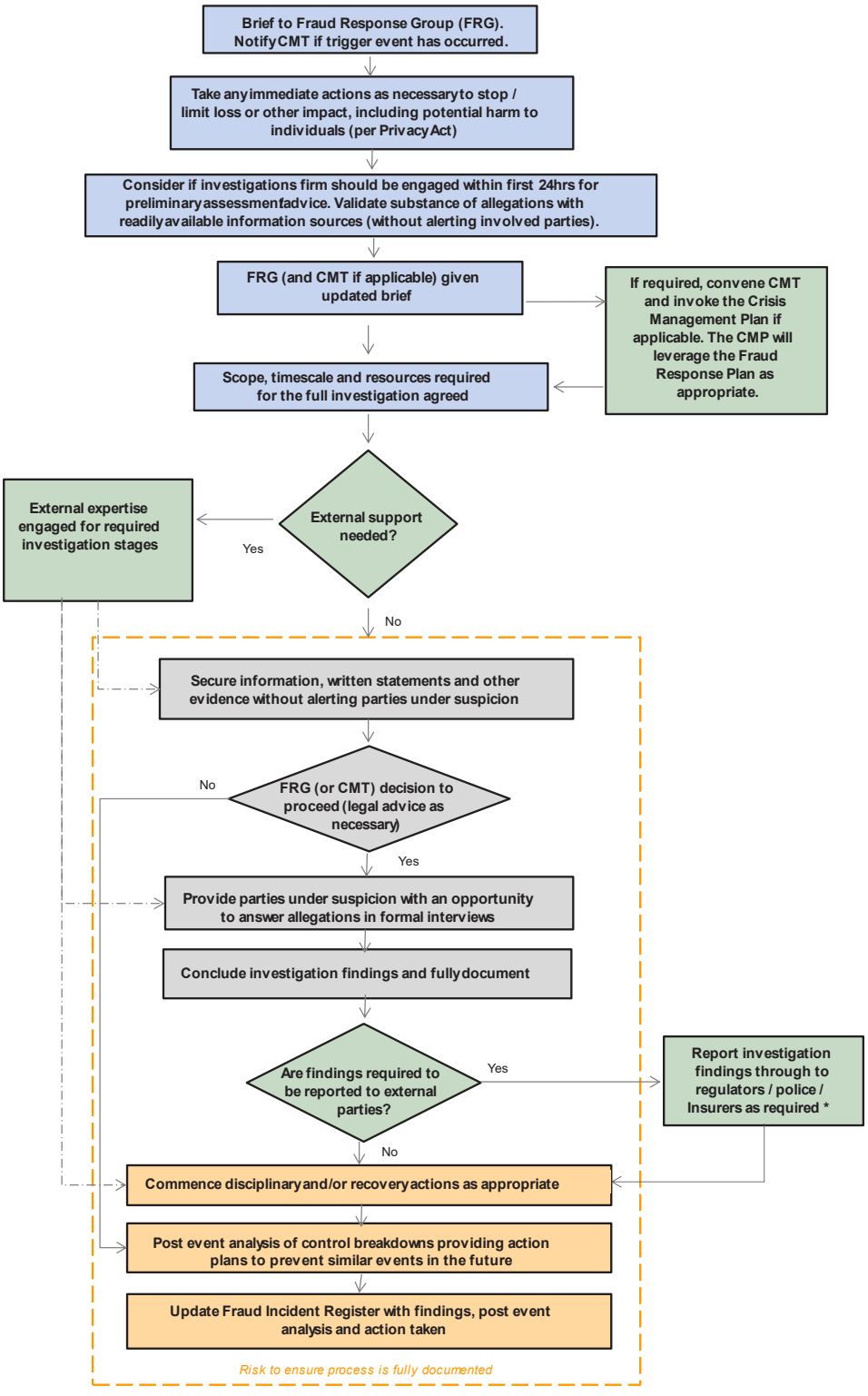
9.3.1 Convening the Crisis Management Team

The FRG may also elect to convene the Crisis Management Team should the matter under investigation have wider implications across the organisation or present the potential for adverse legal or media responses.

9.3.2 External Support

Where potential severity warrants additional expertise, external forensic support will be made available, at the discretion of the Fraud Response Group, to the investigation in order to ensure information / evidence gathering and the processes followed preserve the admissibility of evidence and do not compromise any further disciplinary or recovery actions (‘digital evidence first response’). External parties engaged to provide support to a fraud investigation will be subject to a binding agreement in relation to the release of confidential information coming into their possession during the course of the investigation.

9.4 Procedures for the Fraud and Corruption Response Plan



* AML / CTF Suspicious Matter Reporting, privacy breach reporting and/or CPS243 reporting may also have been triggered at earlier points in the process

9.4.1 Securing Information

Information and evidence gathered as part of a fraud and/or corruption incident investigation may include:

- invoices, statements or payment details
- relevant witness statements
- documentary evidence
- telephone records
- computer system records
- tracing funds / assets / goods
- enquiries with third parties
- interviews with persons suspected of involvement in fraud and corruption (once the FRG has decided to proceed to this stage).

Investigations are conducted in accordance with the principles of natural justice and with a view to determining the facts of the incident. Evidence is gathered in a controlled and legal manner. It is the responsibility of the FRG to ensure that proper records are maintained including accurate notes of when, where and from whom evidence was obtained and by whom.

9.4.2 Internal reporting and escalation

Confirmed fraud and corruption incidents, regardless of materiality are captured in the Group Incident Register (maintained in the BRiskWise system). The register contains the following minimum information in relation to every reportable fraud and corruption incident:

- Date and time of report
- Date and time that incident was detected
- How the incident came to the attention of management (e.g. anonymous report, normal report, supplier report)
- The nature of the incident
- Value of loss (if any) to the entity
- The action taken following discovery of the incident

The FCR team also maintains details of fraud and corruption investigations, including potential or confirmed cases of fraud and corruption.

Summarised reporting and analysis will be provided periodically to the GRC as part of risk management reporting.

9.5 Consequences for fraud and corruption

Any behaviour of a kind that involved an act of fraud and / or corruption would breach at a minimum the Challenger Code of Conduct requirement to act honestly and display a high level of integrity. Failure to comply with this Code of Conduct or this Policy (including any attempt to threaten or cause harm to another employee who is responsible for investigating potential internal fraud) will be dealt with in accordance with Challenger's CRCM Framework, and could result in Challenger taking disciplinary action against the individual including termination of employment.

Bribery and corruption offences (including those relating to bribery of foreign public officials) carry significant penalties in Australia and overseas, as do fraud-related offences set-out under state and federal laws. Beyond adverse impacts to communities in which it occurs, breaches of relevant legislation can have significant impacts for both Challenger and its employees. For Challenger, it may result in legal or regulatory action including criminal proceedings, revocation of license, financial loss and significant reputational damage. Employees may also be subject to civil and criminal proceedings, resulting in financial penalties and imprisonment.

9.6 External reporting

On reaching a finding that there is clear evidence of fraudulent or corrupt activity, the FRG will determine the appropriate law enforcement or regulatory agencies that require notification (with the exclusion of AUSTRAC where obligations are managed under the relevant AML/CTF Program). Challenger has supporting procedures to this Policy that guide the FRG in assessing and determining whether a matter should be reported to the police following the activation of the Fraud Response

Plan. For matters that do not trigger the Fraud Response Plan, the process should be followed by the Head of FCR as part of considering external reporting obligations under the Incident Management Policy.

OAIC notification

Challenger's Internal Privacy Policy outlines when the Office of the Australian Information Commissioner (or any affected individual) would be required to be notified where an incident of fraud also involves a privacy breach. Consideration will also be given to whether Challenger has any contractual obligation to inform particular third parties of the activity.

For example, if the fraudulent or corrupt activity involves a data breach relating to personal information held by Challenger on behalf of a third party under contract, the matter will be notified to the third party in accordance with any contractual obligations.

APRA notification

Under APRA's CPS234 Information Security, regulated entities are required to notify APRA about certain 'information security incidents' and 'information security control weaknesses' within specified timeframes.

For *information security incidents,* APRA must be notified as soon as possible, or in any case, no later than 72 hours after becoming aware of an incident that:

- materially affected, or had the potential to materially affect (financially or non-financially) the entity or the interests of depositors, policy holders, beneficiaries or other customers; or
- has been notified to other regulators, either in Australia or other jurisdictions

For *control weaknesses*, APRA must be notified as soon as possible and, in any case, no later than 10 business days, after becoming aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.

This means that a fraud event will be reportable to APRA if:

- it involved a material information security incident as defined above; or
- it revealed a material information security control weakness which can't be remediated promptly; or
- the information security incident was reported to the OAIC under the privacy breach notification regime

External Reporting requirements are considered as part of the Fraud Response Plan process, outlined in section 9.4

9.7 Civil proceedings and recovery of the proceeds of fraud and corruption

Challenger is committed to fostering an organisational culture which will ensure that the effective prevention of fraud and / or corruption is an integral part of operating activities, with potential instances of fraud and/or corruption promptly investigated once reported. Challenger may choose to pursue legal remedies available under the law as appropriate.

9.8 Internal control review following discovery of fraud

In each instance where potential fraud and / or corruption is confirmed, the Risk and Compliance team, in conjunction with relevant management, will reassess the adequacy of the internal controls (particularly those directly impacting on the fraud incident and potentially allowing it to occur), and as appropriate amend and improve the controls as soon as possible.

9.9 Group Insurance Program

Challenger maintains a Group insurance program. The Insurance program is regularly reviewed and includes consideration of fraud, corruption and theft of Challenger property and for relevant businesses fidelity guarantee insurance. The Fraud Incident register may be reviewed as input to the insurance program renewal process.

The FRG will consider and report as required the details of a confirmed fraud incident to Company Secretary in line with the terms of the Group Insurance Program.

10. Training and Awareness

Training is currently delivered as part of induction and online Risk and Compliance training provided to Challenger employees. The Financial Crime Risk team is also responsible for the design and delivery of targeted face-to-face training sessions on a periodic basis. Such training will typically focus on higher-risk processes or learning opportunities arising from fraud-related incidents.

11. Risk Appetite and complying with this policy

Challenger's vision is to provide our Customers with financial security for retirement. Challenger promotes a positive culture of risk awareness and transparency, including open communication and challenge of current and emerging risks, speaking up regarding matters of concern and the proactive management of issues and incidents. Challenger has no appetite for conducting business activities unfairly or in contravention of the law, or which knowingly damage or are inconsistent with its brand and reputation. Challenger has no appetite for employees intentionally not following policies and procedures.

Employees are to comply with Challenger policies and are responsible for familiarising themselves with the policies relevant to their role. Policies are available on the intranet.

Incidents of non-compliance with this policy are to be reported in line with the Challenger Incident Management Policy.

Employees at Challenger are held accountable for their actions. Consequences for non-compliance with this Policy may include but are not limited to:

- a requirement to undertake additional training
- increased supervisions
- a verbal warning
- a written warning (including a first and final written warning)
- an impact to performance rating or promotion
- a financial consequence
- dismissal.

12. Point of Contact

The key contact on all matters relating to this policy is the Head of FCR.

13. Review Cycle

This Policy will be reviewed and updated as required due to business and external considerations and at least every two years. This Policy is subject to periodic review by Internal Audit (according to Challenger's Internal Audit Program), and elements of the framework will also be monitored by Risk and Compliance periodically in accordance with the broader Line 2 Assurance Program. Any policy recommendations arising from monitoring activities will be considered and implemented as appropriate, which may require an out-of-cycle review.

Supporting procedures to this Policy are of a more dynamic nature and will be updated and amended on a periodic basis or as deemed necessary by the Head of FCR.