



Scams Prevention Policy

Template





ASFA has been operating since 1962 as the peak policy, research and advocacy body for Australia's superannuation industry. ASFA represents the APRA regulated superannuation industry with over 100 organisations as members from corporate, industry, retail and public sector funds, and service providers.

We develop policy positions, service standards and practice guidance through collaboration with our diverse membership base and use our deep technical expertise and research capabilities to assist in advancing superannuation and retirement outcomes for Australians.

The Association of Superannuation Funds of Australia Limited (ASFA)

PO Box 1485, Sydney NSW 2001

T +61 2 9264 9300 or 1800 812 798 (outside Sydney)

ABN 29 002 786 290

ACN 002 786 290

This material is copyright. Apart from any fair dealing for the purpose of private study, research, criticism or review as permitted under the Copyright Act, no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission.

Enquiries are to be made to The Association of Superannuation Funds of Australia Limited.

www.superannuation.asn.au

© ASFA 2025

Contents

1. Introduction	3
2. Overview	5
Application	5
Background and context	5
Operational and legal context	5
Role of the board and senior management	7
Scam Typology & Indicators	8
3. Policy principles	10
Allocation of responsibility	10
Risk identification	10
Mitigation	10
Communication and cooperation	10
Iteration	11
4. Policy Statements	12
Key terms and definitions	12
Governance	12
Prevention	13
Detection	13
Reporting	14
Disrupting	15
Responding	16
5. Appendix	17

Introduction

This document has been prepared to assist Trustees in developing a coherent and fit-for-purpose approach to scams prevention and management. It brings together the core elements commonly expected within a scams-related policy framework and presents them in a structured format that Trustees may adapt to suit their own operational circumstances.

Trustees can draw on the document in when reviewing or developing their own scams policies and strategies, assessing internal capabilities, or aligning current practices with evolving regulatory expectations.

The framework, principles and examples provided are intended to support consistent interpretation and application, while recognising that organisational structures, service delivery arrangements and member profiles differ across the industry.

This resource may also support internal planning, governance reviews, and engagement with service providers by providing a consolidated reference point for the key components of scams prevention, detection and response.

Trustees should refine or adjust the content to reflect their own operational circumstances or changes in regulatory requirements, operational processes or risk settings.

This resource does not constitute legal advice. It has not been designed to meet, nor has it taken account of, the specific operational requirements of any particular individual or organisation. Suggested policy positions are of a general nature, and should be assessed as part of robust internal framework development and evaluation processes. You may wish to consider seeking legal advice from a qualified professional prior to adopting and implementing suggested measures. While care has been taken to extensively identify applicable Scams-related legal and regulatory obligations, it should not be assumed that this resource is an authoritative or exhaustive consolidation of applicable law. You should seek legal advice if unsure of the precise scope of your obligations from time-to-time.

Overview

Background and context

In February 2025, the Scams Prevention Framework Act 2025 (Cth) became law. The regime, which was added to the Competition and Consumer Act 2010 (Cth), is a world-first, and indeed, world-leading approach to systemically combatting the growing risk that scams pose to the financial security of everyday consumers¹.

Until now, Australia's regulatory approach to combatting scams has been structurally disjointed; as acknowledged by ASIC in recent public remarks².

The great benefit of the Scams Prevention Framework (SPF) is that it delivers a cohesive, thematically stepped-out approach to scam prevention and response. It's at once something borrowed, and something new. Certain requirements relating to remediation, reporting, and governance are aligned with and complement the Financial Accountability Regime (FAR) by requiring boards and executive managers to take a hands-on, iterative, and performance driven approach to managing the frameworks and processes that guard against scams.

The need to maintain accessible reporting mechanisms through which consumers can report actual or suspected scam-related activity is redolent of and intertwined with the existing Internal Dispute Resolution (IDR) framework reflected in ASIC Regulatory Guide 271: Internal Dispute Resolution.

Other features, including the positive obligations to detect scams, report Actionable Scam Intelligence (even where it has not been concluded that a scam has or will occur), and take steps to stop scams from happening, reflect a decisive break from past regulatory posture. Proactive prevention, rather than controlled reactivity, is the order of the day.

The purpose of this policy is to provide a consistent and structured approach to managing the risk of scams to members of the Fund and assist in related statutory obligations.

Operational and legal context

The Scams Prevention Framework is the central pillar of the Australian Government's response to addressing scams.

It sets-out six overarching best-practice principles that imposes broad obligations on entities that operate in sectors that have been designated by the responsible Minister.³

¹ ACCC welcomes passage of world-first scams prevention laws | ACCC

² The times they are a-changin'— but directors' duties aren't | ASIC



The framework is administered by the Australian Competition and Consumer Commissioner (ACCC) as the Scams Prevention Framework Regulator⁴. It is expected that AFCA will be the designated external dispute resolution scheme⁵.

The regime also creates scope for more detailed operational requirements. The Minister is empowered to issue binding rules that apply to all entities across all designated sectors⁶.

The Minister is also empowered to issue binding SPF Codes that impose tailored industry-based obligations on entities within specific designated sectors⁷. The Minister can designate entities other than the ACCC as the regulator responsible for Scams Prevention Framework Code enforcement⁸.

A broad suite of penalty provisions are available in cases of non-compliance.

Civil penalties of up to \$53 million are imposable, together with alternative remedial measures such as public warnings and adverse publicity notices⁹.

Although superannuation funds are not in the first tranche of designated sectors, trustees develop cohesive scams prevention practices that align with the Scams Prevention Framework Code.

APRA and ASIC have separately written to trustees to both convey their view that existing scam management approaches are inadequate, and request immediate uplift¹⁰.

Getting ahead of the regulatory curve by harmonising internal practices with the framework by which RSEs will eventually be governed is a decision that would potentially demonstrate diligence and deliver efficiency dividends when and as

3 Competition and Consumer Act 2010 (Cth) s 58AC.

4 Competition and Consumer Act 2010 (Cth) s 58EB.

5 Competition and Consumer Act 2010 (Cth) s 58DA.

6 Competition and Consumer Act 2010 (Cth) s 58GE.

7 Competition and Consumer Act 2010 (Cth) s 58CB.

8 Competition and Consumer Act 2010 (Cth) s 58ED.

9 Competition and Consumer Act 2010 (Cth) Division 6 – Enforcing the Scams Prevention Framework.

superannuation is made a designated sector.

It is important to remain cognisant of concurrent, pre-existing regulatory obligations that sit adjacent to obligations under the Framework. These are extensively listed within the Appendix to this document.

In the course of both considering the adoption of this policy, and preparing for compliance with the Scams Prevention Framework, trustees might consider how practically equivalent or similar obligations can be synthesised or replicated across multiple policies and internal frameworks.

Role of the board and senior management

As a principles-based regime, the Framework vests regulated entities with extensive latitude to determine the precise details of their approach to implementation.

In fact, the first task allocated to regulated entities (which, in the context of superannuation, will ultimately mean the Trustee, as licence holder) under the principle of 'Governance' is to develop and implement policies, procedures, metrics, and targets that will enable the Trustee to comply with the five operative principles of the framework¹¹.

It is self-evident that trustees cannot treat this as a 'set and forget' exercise. Each year, a Senior Officer will be required to certify that the above items remain compliant with the framework¹².

Internally, trustees will have several new positive obligations. There will be a requirement to identify beneficiaries who are at risk of being targeted by a scam, as well as beneficiaries who have a heightened risk of being targeted by a scam¹³.

Trustees will also need to establish and maintain a Reporting Mechanism through which beneficiaries can convey Actionable Scam Intelligence, and then actively investigate that intelligence even where a Scam has not yet occurred¹⁴.

This requires a systemic approach to triage and evaluation that will likely require structural change and integration. Perhaps most significant is the obligation to take 'reasonable steps' to disrupt and prevent Scams where Actionable Scam Intelligence is received¹⁵.

Trustees will also be required to participate in a whole-of-sector approach to reporting and dealing with Actionable Scam Intelligence.

Presently, there is no binding requirement or mechanism through which trustees share intelligence about confirmed or suspected scams with one another.

Indeed, media coverage is often the only source of such information. Under the

¹⁰ See 'Protecting Australians Against Scams and Fraud ASIC Letter to RSE Trustees, 29 January 2025' and

'For action: Information Security Obligations and Critical Authentication Controls APRA Letter to RSE Trustees, 10 June 2025.'

¹¹ Competition and Consumer Act 2010 (Cth) s 58BD.

¹² Competition and Consumer Act 2010 (Cth) s 58BE.

¹³ Competition and Consumer Act 2010 (Cth) s 58BK(2).

¹⁴ Competition and Consumer Act 2010 (Cth) s 58BN.

¹⁵ Competition and Consumer Act 2010 (Cth) s 58BX.

framework, trustees will be obligated to provide a report on all Actionable Scam Intelligence (even where it has not been confirmed that a scam has or is likely to occur) to the Scams Prevention Framework Regulator¹⁶.

The Regulator can then make the reports available to other regulated entities, or the regulators of other regulated sectors¹⁷.

While the duty to beneficiaries of course remains paramount, the framework marks a shift to an operational mindset that is less siloed and encourages a collective approach to a collective risk.

Scam Typology & Indicators

The below table sets-out the kinds of scams that frequently target superannuation beneficiaries.

The terms ‘scam’ and ‘fraud’ are often used interchangeably. There are definite similarities. However, it is important that a distinction is drawn.

In a recent communication to trustees, ASIC identified ‘fraud’ as the circumstance where an unauthorised transaction occurs without the direct facilitation or assistance of the affected member.

In contrast, a scam involves full or partial facilitation by the member, who is deceived into transferring funds out of their superannuation account to the scammer, or aiding a scammer to make a transfer (e.g. by providing a scammer who may be impersonating the superannuation fund with a one-time password)¹⁸.

This is closely aligned with the definition provided within the Scams Prevention Framework, wherein scam is expansively defined to encompass any direct or indirect attempt to engage a consumer where the attempt involves deception, and would – if successful – occasion harm to that consumer¹⁹.

It follows that an instance of fraud (i.e., a third party logging-in to a member’s account with that member’s credentials and effecting transactions) may have arisen through an element of deceit (i.e., the scammer obtained the details from the member through posing as a representative of the super fund, or holding themselves out as a financial adviser); thereby rendering the circumstance categorizable as a scam.

It is important to remember that the techniques and technologies employed by scammers are constantly changing. Trustees should carefully and ongoingly monitor data and member experiences to expand their knowledge base of Scam methodologies.

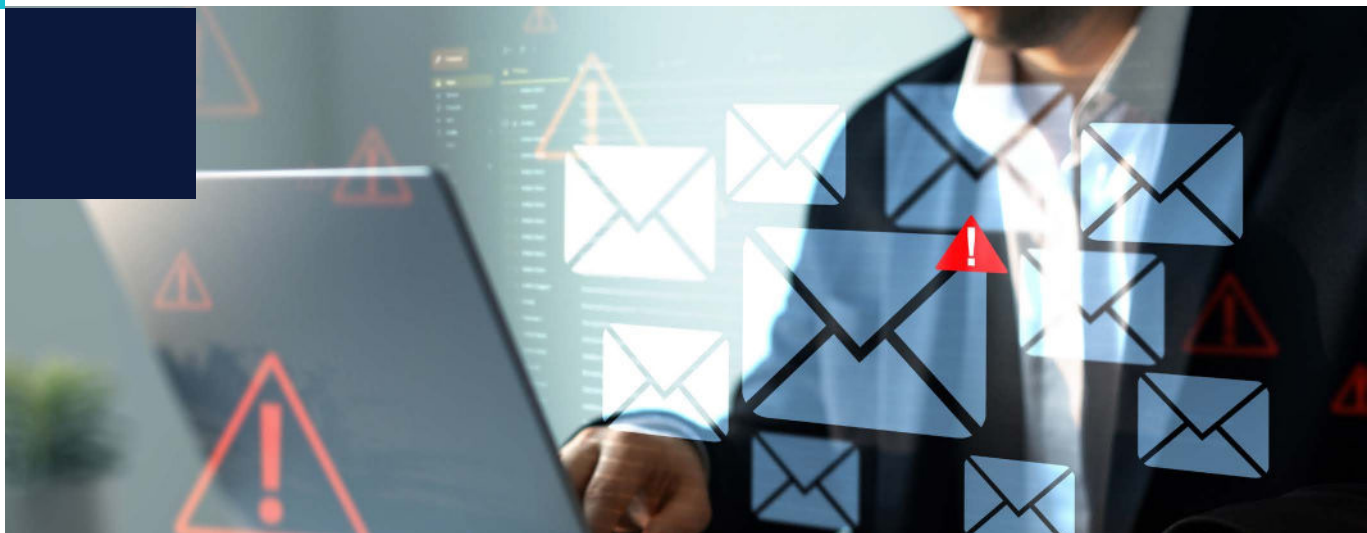
¹⁶ Competition and Consumer Act 2010 (Cth) s 58BR.

¹⁷ Competition and Consumer Act 2010 (Cth) s 58BV.

¹⁸ Protecting Australians Against Scams and Fraud ASIC Letter to RSE Trustees, 29 January 2025.

¹⁹ Competition and Consumer Act 2010 (Cth) s 58AG.

Indicator	Scam Type(s)
A transition to a Self-Managed Super Fund (SMSF) after many years of regular contributions.	Investment
Successive or concurrent requests for withdrawal on compassionate grounds.	Early access
	Early access
Provision of incorrect documents, or which appear forged, falsified, tampered with, or are otherwise fraudulent in relation to payment requests (including insurance claims)	Phishing and identity theft
A large or complete rollover when a member: a) Is approaching preservation age and/or; b) Has a balance that is lower than what is typical or expected for a member in comparable circumstances and/or; c) Has experienced a significant, adverse life event	Early access
	Investment
A large or complete lump sum withdrawal when a member: d) Has recently reached preservation age; and e) Has recently changed contact details; or f) The details of their financial institution ¹	Romance
	Investment
	Romance



While these circumstances may indicate the scams type above, they are not dispositive without further evidence. They are factors which funds should consider but they are not conclusive without more

Policy Principles

The Trustee commits to giving effect to these fundamental principles in its approach to managing the risk and impact of scams, and in implementing any measures that arise under the Scams Prevention Framework.

Allocation of responsibility

The Trustee will identify the functions and responsibilities that are required to implement a comprehensive approach to scams management.

The Trustee will develop clear lines of accountability that attach to each identified function and responsibility. Where possible, overarching responsibility will be expressly vested in a Senior Executive Manager.

Risk identification

The Trustee identifies scams as a risk for the purpose of its Risk Management Framework.

The Trustee recognises the varied modality of scams and commits to developing different categories into which actual or reasonably foreseen kinds of scams may be categorised; based on the likelihood of and gauged impact on beneficiaries if the Scam occurred.

The Trustee acknowledges that beneficiaries may be susceptible to scams based on personal attributes and circumstances. It will develop risk metrics that assist in rating the scam related risk profile of individual beneficiaries.

Mitigation

The Trustee's Risk Management Framework will include the identification and development of controls to mitigate the risk of Scam events adversely impacting the Trustee and beneficiaries.

The Trustee will seek to develop controls for each risk-profiled cohort of members that can be implemented to minimise the risk of Scams, interrupt Scams where there is reason to believe a scam may actually occur, and respond to harm where a Scam does occur.

Communication and cooperation

The Trustee will be open in sharing Actionable Scam Intelligence with regulators, and where appropriate, industry peers.

The Trustee will make resources publicly available and may participate in Scam intelligence Reporting Mechanisms. Where it has assessed a foreseeable risk of significant harm occurring to risk-profiled members resulting from Scam activity, the Trustee will take steps to prevent a likely scam from being carried out. This may include notifying the beneficiary.

Where a scam occurs, the Trustee will provide assistance and support to victim beneficiaries and provide resources that detail support services and thoroughly describe available IDR and EDR pathways.

Iteration

The Trustee will set targets for the management of Scams risk.

The Trustee will annually review the effectiveness of its scams management control environment, with reference to targets as well as the evolving legislative and regulatory obligations and Scam threat landscape.



Policy Statements

Key terms and definitions

Defined terms used throughout this document have the meaning accorded by law from time-to-time.

Governance

The Trustee identifies the risk of Scam events against beneficiaries as a risk for the purpose of the Trustee's risk management framework²⁰.

The Trustee will set annual performance metrics and targets that emphasise continuous improvement by aspiring to year-on-year improvement in scams²¹.

The Trustee will ensure the preparation of a regular report on its performance against scam related risk appetite, targets, and benchmarks²².

The Trustee will designate the Annual Certification process of Scams Prevention Framework policies, procedures, metrics, and targets as a 'Key Function' of a specific 'Accountable Person' within Financial Accountability Regime (FAR) frameworks²³.

The Trustee will ensure that the findings of regular reviews of proposed benchmarks inform and are referenced within the senior officer's Annual Certification²⁴.

The Trustee will define a targets and metrics underperformance threshold which will require an internal review of policies and procedures²⁵.

The Trustee will ensure that the Annual Certification specifies and incorporates new performance metrics and targets for the forthcoming year²⁶.

The Trustee will seek regular confirmation from its administrator and service providers that the processes, protocols, and infrastructure employed by the service provider responsible for the direct provision of services to members are consistent with the Trustee's Scams Prevention Framework policies, procedures, targets, metrics, and the provisions of any Scams Prevention Framework Rules or Scams Prevention Framework Codes.

The Trustee will take all reasonable steps to ensure that data held or collected by external administrators is provided to the Trustee for the purpose of regular benchmark assessment. Where underperformance triggers a review, the Trustee will take all reasonable steps to ensure the cooperation of its external administrator in the course of that review²⁷.

²⁰ Superannuation Prudential Standard 220: Risk Management [5] – [6].

²¹ Competition and Consumer Act 2010 (Cth) s 58BD(1)(c).

²² Competition and Consumer Act 2010 (Cth) s 58BD(1)(c).

²³ Competition and Consumer Act 2010 (Cth) s 58BE(1)(a) – (b).

²⁴ Ibid.

²⁵ Ibid.

²⁶ Ibid.

²⁷ Protecting Australians Against Scams and Fraud ASIC Letter to RSE Trustees, 29 January 2025.

Prevention

The Trustee is committed to managing the risk of scam activity within its stated risk appetite. Preventative controls will be adopted as part of the Trustee's risk management framework, in conjunction with its administrator and service providers where required, and regularly reviewed and tested for effectiveness²⁸.

All beneficiaries are considered to be at risk of being targeted by scams, and the Trustee will take steps to identify beneficiaries that may be more vulnerable to scams in general or to certain types of Scams²⁹.

The Trustee's Risk Appetite Statement (RAS) must include an appetite for material risk(s) that relate to Scam risk³⁰.

Optionally, The Trustee must set a risk appetite for Scam risk specifically in its RAS.

The Trustee – in conjunction with its administrator – will ensure that scam-related policies and procedures are not restricted to fraud, and that legitimate yet anomalous member activity (including a cessation of regular contributions and payments, a rollover, or large lump sum withdrawal) is flagged as a potential indicator of scam-related activity³¹.

The Trustee will ensure that multi-factor authentication (MFA) or similar controls are in place for all scam risk-related activities (such as changing member details, withdrawals, benefit payment / transfer / rollover requests, or investment switching)³².

Detection

The Trustee will establish and maintain detective controls that are designed to identify Actionable Scam Intelligence. Such controls will apply at the time of the activity, and after the activity is complete³³.

The Trustee will designate the investigation of Actionable Scam Intelligence as a 'Key Function' of a specific 'Accountable Person' within FAR frameworks³⁴.

As part of investigations into Actionable Scam Intelligence, the Trustee will:

1. Identify designated cohorts of beneficiaries who are likely to be affected by the possible scam, based on the nature and scope of the prospective scam that is reflected in the Actionable Scam Intelligence
2. Review the recent activity and transactions of all or a sample group from beneficiary cohorts deemed at-risk to inform the investigations of Actionable Scam Intelligence
3. Evaluate the benefit in directing communications to all or some members of a designated beneficiary cohort to warn of possible Scam activity³⁵.

²⁸ Competition and Consumer Act 2010 (Cth) s 58BJ(1).

²⁹ Competition and Consumer Act 2010 (Cth) s 58BK(2)(b).

³⁰ Superannuation Prudential Standard 220 Risk Management [19] – [20].

³¹ For action: Information Security Obligations and Critical Authentication Controls APRA Letter to RSE Trustees, 10 June 2025

³² Ibid.

³³ Competition and Consumer Act 2010 (Cth) s 58BM(1) – (3).

³⁴ Competition and Consumer Act 2010 (Cth) s58BN(1).

³⁵ Competition and Consumer Act 2010 (Cth) s58BO(1).

³⁶ ASIC Regulatory Guide 277: Consumer Remediation [47][a] – [e].

The Trustee will ensure that investigations into Actionable Scam Intelligence will:

1. Use data, complaints, trend analysis, and known risk indicators to investigate whether beneficiaries have already, or are likely to have already, been affected by the prospective scam.
2. Establish a dedicated liaison with administrators or any external service providers that may have been directly or indirectly involved in the possible scam³⁶.

Reporting

The Trustee will maintain a record of all Scam intelligence reported to it by beneficiaries and prospective beneficiaries through the mandatory Scams Reporting Mechanism for no less than six years. The record will be retained in a central register of reported Scam intelligence. Information held in the register will be consulted as part of the Annual Certification of Scams Prevention Framework polices, procedures, metrics, and targets³⁷.

The Trustee will maintain a separate register of all Actionable Scam Intelligence found to relate to an actual Scam and keep a record of this intelligence for no less than six years. Information held in the register will be consulted as part of the Annual Certification of Scams Prevention Framework polices, procedures, metrics, and targets³⁸.

The Trustee will ensure that a scam prevention and response function is maintained and adequately resourced OR that a dedicated scam prevention and response function is maintained and adequately resourced. The function must enable continuity of complaints management to be achieved even where changes in individual case managers or other responsible personnel occurs. It must also require the cooperation of Service Providers to the extent that this is operationally required³⁹.

The Trustee designates the overall handling of scam-related Complaints as a 'Key Function' of a specific 'Accountable Person' within FAR frameworks⁴⁰.

Disrupting

The Trustee will develop operating procedures, in conjunction with Service Providers and its administrator where necessary, to ensure reasonable steps can be taken to disrupt scams where Actionable Scam Intelligence is held or verified. This may include, but is not limited to:

1. Immediate referral to other Government and law enforcement agencies, including the AFP, AUSTRAC, and ATO
2. Placing a hold on the activity of individual beneficiaries, or cohorts of beneficiaries, until further investigation of a relevant Scam has been undertaken

³⁶ ASIC Regulatory Guide 277: Consumer Remediation [47][a] – [e].

³⁷ Superannuation Prudential Guide 223 Fraud Risk Management [24][b].

³⁸ Protecting Australians Against Scams and Fraud ASIC Letter to RSE Trustees 29 January 2025.

³⁹ Regulatory Guide 271 Internal Dispute Resolution [179] – [180].

⁴⁰ Ibid.

3. Issuing cautionary communications to individual beneficiaries, or cohorts of beneficiaries, based on the nature of Actionable Scam Intelligence
4. Cross-referencing the payee details of requested transactions to determine if withdrawals are directed to financial institution accounts that match current member records OR
5. Cross-referencing the USIs or SPINs that attach to requested rollovers to determine risk level⁴¹.

Responding

The Trustee will adopt a multi-channel Reporting Mechanism through which members (and member close associates) can report Scam-related activity. This may include, but not be limited to:

1. Independent third-party representative
2. Web-based portals
3. Hotlines
4. A postal address⁴².

The Trustee will provide and promote the availability of services that can support members in making a Complaint, including but not limited to:

1. LOTE or AUSLAN interpreters
2. Support staff with training in and understanding of First Nations kinship and cultural practices⁴³.

The Trustee will develop and provide an accessible resource to complainants that:

1. Outlines the steps that form part of the IDR process (including the possibility of the complainant referring the matter to AFCA at the conclusion of the IDR process)
2. Identifies the mandatory timelines that govern the Trustee's overall handling of the Complaint, as well as individual itemised steps. Where different, identify the internal processing target set by the Trustee.
3. Provides a link to an online portal and/or contact details through which complainants can review the status of their Complaint including progress-to-date and forthcoming steps.
4. Advises members to consider seeking financial and psychological counselling, and provides pathways for accessing those services⁴⁴.

The Trustee will make information about its handling of Scam activity available on its public website. Pursuant to this commitment, the Trustee will consider publishing this Policy on its public website⁴⁵. The Trustee will prepare a version of this Policy that is drafted in plain English and structured to enhance navigability and intelligibility for members without technical subject matter expertise.

⁴¹ Competition and Consumer Act 2010 (Cth) s 58BX(1)(b) and 58BZA(2)(c) – (d).

⁴² Competition and Consumer Act 2010 (Cth) s 58BZ(1).

⁴³ Ibid.

⁴⁴ Competition and Consumer Act 2010 (Cth) s 58BZD(1)(a).

⁴⁵ Competition and Consumer Act 2010 (Cth) s58BZF(1).

The Trustee will assess the modes of regular member communications best-suited for publicly communicating its Scam Reporting Mechanism, Internal Dispute Resolution Scheme, and External Dispute Resolution arrangements⁴⁶.

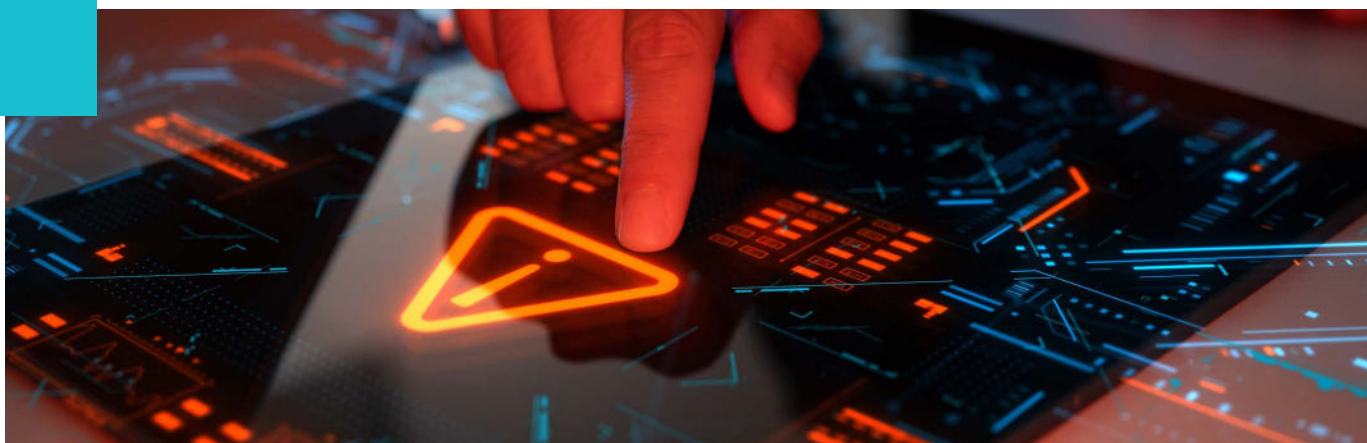
The Trustee will assess an appropriate frequency at which to feature this information in member communications⁴⁷.

The Trustee will maintain a Scam Remediation Framework for use in circumstances where:

A scam has occurred and caused financial detriment to a member or the fund;
and

1. The Trustee's IDR has determined that an action or omission of the Trustee that does not comply with its legal obligations or internal policy procedures has fully or partially contributed to the member's loss.
2. Among other things, the framework will assess:
3. The extent to which the Trustee complied with obligations under Scams Prevention Framework (including Scams Prevention Framework Rules and Scams Prevention Framework Codes) and its own Scams Prevention Framework policies and procedures at the time the scam occurred; and
4. The nature and scope of any member's loss
5. The member's proximity to retirement and capacity to recontribute lost amounts
6. The prospect of the loss being recouped through legal enforcement or other means.
7. Whether, if applied uniformly in like circumstances, the compensatory allocation of units to the affected member would be unfair or cause unacceptable financial detriment to other beneficiaries⁴⁸.

Trustees need to ensure they liaise with banks when assessing compensation requests to ensure payments are made by the correct entity.



⁴⁶ Ibid.

⁴⁷ Ibid.

⁴⁸ ASIC Regulatory Guide 277: Consumer Remediation [68].

Appendix

The following appendix itemises broader legal and regulatory obligations that may inform the Trustee's Scams Prevention Policy and other Scams Management practices and procedures from time-to-time.

The appendix follows the structure of the Policy insofar as obligations are organised in accordance with the principles of the Scams Prevention Framework.

While care has been taken in the preparation of the resource, it should not be seen as exhaustive or authoritative. If you are unsure of your obligations, seek legal advice.

Governance	
<p>Competition and Consumer Act 2010 (Cth) s 58BD(1)(a) – (b).</p>	<p>The Trustee should document and then implement governance and policy procedures about:</p> <ul style="list-style-type: none"> a) Preventing, detecting, and disrupting scams; and b) Responding to scams; and c) Reports relating to scams.
<p>Superannuation Prudential Standard 220: Risk Management [5] – [6].</p>	<p>The Trustee should at all times have a risk management framework to appropriately:</p> <ul style="list-style-type: none"> a) Manage the risks to its business operations; and b) Enable the Trustee to develop and implement strategies, policies, procedures and controls to appropriately manage different types of material risk.
<p>Competition and Consumer Act 2010 (Cth) s 58BD(1)(c).</p>	<p>The Trustee should develop and implement performance metrics and targets that:</p> <ul style="list-style-type: none"> a) Measure the effectiveness of governance and policy procedures; and b) Comply with prescribed requirements in SPF rules.

Governance	
<p>Competition and Consumer Act 2010 (Cth) s 58BE(1)(a) – (b).</p>	<p>The Trustee must ensure a senior officer certifies in writing:</p> <ul style="list-style-type: none"> a) Within 12-months of the day on which the entity becomes a regulated entity; and b) Within 7 days of each 12-month anniversary thereafter <p>That all policies, procedures, metrics, and targets comply with the SPF framework.</p>
<p>Superannuation Prudential Standard 220: Risk Management [27] and [28].</p>	<p>The Trustee should ensure that the appropriateness, effectiveness, and adequacy of its risk management framework are subject to a comprehensive review by operationally independent, appropriately trained and competent persons at least every three years.</p> <p>The Trustee must also undertake, for each year during which a comprehensive review does not take place, a review of the appropriateness, effectiveness and adequacy of the risk management framework.</p>
<p>Financial Accountability Regime (Minister) Rules 2024 s 5(2) (c),(e), and (g) and s 8(2)(a).</p>	<p>The Trustee must allocate senior executive responsibility for management of the accountable entity’s overall</p> <ul style="list-style-type: none"> a) Risk controls or overall risk management arrangements; b) Dispute resolution function (whether internal or external, or both); c) Management of breach reporting; d) member administration operations.
<p>Superannuation Prudential Standard 220: Risk Management [16][e].</p>	<p>The Trustee should develop clearly defined and documented roles, responsibilities and formal reporting structures for the management of material risks throughout business operations.</p>

Governance	
<p>Competition and Consumer Act 2010 (Cth) s 58BF(1).</p>	<p>The Trustee must retain, for a period of 6 years, records of information that materially relates to:</p> <ul style="list-style-type: none"> a) The creation of, modifications to, and/or the annual recertification of policies, procedures, metrics, and targets; and b) The implementation of policies, procedures, metrics, and targets; and c) Certification and annual re-certification of those policies, procedures, metrics, and targets
<p>Superannuation Prudential Guide 223: Fraud Risk Management [6].</p>	<p>The Trustee should maintain a risk management framework that includes a framework for the management of fraud risk.</p> <p>The Trustee should ensure this framework addresses the risks arising from both internal fraud and external fraud in a manner that is commensurate with the broader risk management framework and which reflects the size, business mix and complexity of business operations.</p>
<p>Superannuation Prudential Guide: 223 Fraud Risk Management [18].</p>	<p>The Trustee should institute active stewardship by senior management of the planning, execution and ongoing maintenance of the fraud risk management framework. This includes periodic consideration of whether the fraud control plan is meeting its objectives and whether the measures implemented are addressing the identified risks across the entirety of the RSE licensee's business operations.</p>
<p>Superannuation Prudential Standard 220: Risk Management [16][e].</p>	<p>The Trustee should develop clearly defined and documented roles, responsibilities and formal reporting structures for the management of material risks throughout business operations.</p>

Governance	
<p>Superannuation Prudential Guide 223: Fraud Risk Management [24][e]</p>	<p>The Trustee should maintain a fraud control plan that documents:</p> <ul style="list-style-type: none"> a) Fraud risks; b) Person(s) responsible for fraud risk controls; c) Key fraud indicators that fraud risk controls are designed to detect; d) Processes to follow when reporting a fraud related concern, including how a subsequent investigation would be conducted; and e) Fraud risk management training to be provided.
<p>Cross Prudential Standard 230: Operational Risk Management [12].</p>	<p>The Trustee must effectively:</p> <ul style="list-style-type: none"> a) Manage operational risks, and set and maintain appropriate standards for conduct and compliance; b) Maintain critical operations within tolerance levels through severe disruptions; and c) Manage the risks associated with the use of service providers.
<p>Cross Prudential Standard 230: Operational Risk Management [15].</p>	<p>The Trustee must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks.</p>
<p>Cross Prudential Standard 230: Operational Risk Management [16].</p>	<p>The Trustee must develop and maintain governance arrangements for:</p> <ul style="list-style-type: none"> a) The oversight of operational risk; and b) An assessment of its operational risk profile, with a defined risk appetite supported by indicators, limits and tolerance levels.

Governance	
<p>Cross Prudential Standard 230: Operational Risk Management [21] – [22].</p>	<p>The Trustee must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior managers for operational risk management, including business continuity and the management of service provider arrangements.</p> <p>The Trustee must also oversee operational risk management and the effectiveness of key internal controls in maintaining the entity’s operational risk profile within risk appetite. The Board must be provided with regular updates on the APRA-regulated entity’s operational risk profile and ensure senior management takes action as required to address any areas of concern.</p>
<p>Cross Prudential Standard 234: Information Security [18].</p>	<p>The Trustee must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.</p>
<p>Cross Prudential Standard 234: Information Security [20].</p>	<p>The Trustee must classify information assets, including those managed by related parties and third parties, by criticality and sensitivity. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.</p>
<p>Protecting Australians Against Scams and Fraud ASIC Letter to RSE Trustees 29 January 2025.</p>	<p>The Trustee must maintain sufficient oversight of external administrators’ anti-scams and anti-fraud practices.</p>

Governance	
Protecting Australians Against Scams and Fraud ASIC Letter to RSE Trustees 29 January 2025.	<p>The Trustee must maintain:</p> <ul style="list-style-type: none"> a) A scams strategy; b) Dedicated reporting on scams; and c) Reviewed scam prevention, detection and response capabilities.
Regulatory Guide 271: Internal Dispute Resolution [48].	<p>The Trustee must ensure that outsourced Internal Dispute Resolution processes:</p> <ul style="list-style-type: none"> a) Have measures in place to ensure that due skill and care is taken in choosing suitable service providers; b) monitor the ongoing performance of service providers; and c) appropriately deal with any actions by service providers that breach service level agreements or fall short of their obligations under this regulatory guide.
Regulatory Guide 271: Internal Dispute Resolution [118].	<p>The Trustee must set clear accountabilities for complaints handling functions, including the management of systemic issues identified through consumer complaints.</p>

Prevent	
Competition and Consumer Act 2010 (Cth) s 58BJ(1).	<p>The Trustee must take reasonable steps to prevent another person from committing a scam connected with, related to, or using a regulated service of the entity¹.</p>
Competition and Consumer Act 2010 (Cth) s 58BK(2)(b).	<p>The Trustee must identify:</p> <ul style="list-style-type: none"> a) Beneficiaries who are at risk of being targeted by a scam; and b) Beneficiaries who have a higher risk of being targeted by a scam.

¹ Reasonable steps will be given clearer meaning through SPF Rules and SPF Code(s). See Competition and Consumer Law Act 2010 (Cth) s 58BK.

Prevent	
<p>Superannuation Prudential Standard 220: Risk Management [19] – [20].</p>	<p>The Trustee must maintain an up-to-date risk appetite statement that covers business operations and each category of material risk. The risk appetite statement must be approved by the Board and articulate:</p> <ul style="list-style-type: none"> a) The degree of risk that the Trustee is prepared to accept in pursuit of its strategic objectives and business plan, giving consideration to the interests of beneficiaries (risk appetite); b) For each material risk, the maximum level of risk that the Trustee is willing to operate within expressed as a risk limit that, where possible, is based on a measurable limit of the risk remaining, after taking into account the mitigants for the risk where appropriate (risk tolerance); c) The process for ensuring that risk tolerances are set at an appropriate level, based on an estimation of the impact on the interests of beneficiaries in the event that a risk tolerance is breached and the likelihood that each material risk is realised; d) The process for monitoring compliance with each risk tolerance and taking appropriate action in the event of a breach of the Trustee’s risk tolerance; and e) The timing and process for review of the risk appetite and risk tolerances.

Prevent	
<p>Superannuation Prudential Standard 220: Risk Management [20][b][i] – [v].</p>	<p>The Trustee must maintain a Risk Management Strategy that describes the policies and procedures dealing with the following risk management matters, including the date when each policy or procedure was last revised, the date that it is next due for review and who is responsible for the review:</p> <ul style="list-style-type: none"> a) The processes for identifying and assessing material risks and controls b) The process for establishing, implementing and testing mitigation strategies and control mechanisms for material risks c) The process for monitoring, communicating and reporting risk issues, including escalation procedures for the reporting of material events and incidents d) The mechanisms in place for monitoring and ensuring ongoing compliance with all prudential requirements.
<p>Superannuation Prudential Guide 223: Fraud Risk Management [15].</p>	<p>The Trustee should develop a suite of fraud risk controls that are designed to prevent fraud from occurring, to detect fraud when it occurs and to respond to fraud as it is detected.</p>
<p>Cross Prudential Standard 230: Operational Risk Management [14].</p>	<p>To the extent practicable, the Trustee should prevent disruption to critical operations, adapt processes and systems to continue to operate within tolerance levels in the event of a disruption, and return to normal operations promptly once a disruption is over.</p>

Prevent	
<p>Cross Prudential Standard 230: Operational Risk Management [27].</p>	<p>The Trustee must test the effectiveness of information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with:</p> <ul style="list-style-type: none"> a) The rate at which the vulnerabilities and threats change; b) The criticality and sensitivity of the information asset; c) The consequences of an information security incident; d) The risks associated with exposure to environments where the APRA-regulated entity is unable to enforce its information security policies; and e) The materiality and frequency of change to information assets.
<p>For action: Information Security Obligations and Critical Authentication Controls APRA Letter to RSE Trustees, 10 June 2025.</p>	<p>The Trustee must avoid being overly reliant on anti-fraud measures and having limited focus on the specific risks and harms associated with scams. The Trustee should not only focus on confirming that the person requesting a transfer is the member, rather than looking for flags to indicate that the member may have been tricked.</p>
<p>For action: Information Security Obligations and Critical Authentication Controls APRA Letter to RSE Trustees, 10 June 2025.</p>	<p>The Trustee must require MFA or equivalent controls for all high-risk activities (such as changing member details, withdrawals, benefit payment / transfer / rollover requests, or investment switching) and for all administrative or privileged access. Solutions should consider accessibility for disadvantaged groups or those who may legitimately opt-out of certain digital channels.</p>

Detect	
Competition and Consumer Act 2010 (Cth) s 58BM(1) – (3).	<p>Take reasonable steps to detect a scam relating to, connected with, or using a service:</p> <ul style="list-style-type: none"> a) As it happens; and/or b) After it happens².
Competition and Consumer Act 2010 (Cth) s58BN(1).	<p>Where actionable scam intelligence is received or held, the Trustee must ensure that:</p> <ul style="list-style-type: none"> a) Reasonable steps are taken to investigate whether or not the activity is a scam within 28-days after intelligence becomes actionable scam intelligence.
Competition and Consumer Act 2010 (Cth) s58BO(1).	<p>Where actionable scam intelligence is received or held, the Trustee must ensure that reasonable steps are taken to identify beneficiaries who are or may have been impacted by the activity that is potentially a scam.</p>
Superannuation Prudential Guide 223: Fraud Risk Management [24][a].	<p>The Trustee should conduct regular fraud risk assessments that reflect policies and processes governing initial and ongoing assessment of fraud risks.</p>
Superannuation Prudential Guide 223: Fraud Risk Management [24][d][ii].	<p>The Trustee should issue internal communication that is complementary to training, for example when incidents occur or when a new fraud risk emerges.</p>

² Reasonable steps will be given clearer meaning through SPF Rules and SPF Code(s). See Competition and Consumer Law Act 2010 (Cth) s 58BP.

Detect	
<p>Superannuation Prudential Guide 223: Fraud Risk Management [28][a] – [b].</p>	<p>The trustee should employ a combination of both proactive and reactive detection controls, where:</p> <ul style="list-style-type: none"> a) Proactive controls are periodic measures designed to actively seek out evidence of fraudulent activity and allow objective assessment of the effectiveness of the fraud risk controls in place. Proactive controls detect and address fraud, but also, in instances where no fraud is detected, provide assurance that fraud is being effectively controlled; and b) Reactive controls are tools or systems designed to identify indicators of fraud, to detect fraud when it has occurred, and are typically structured as part of an RSE licensee’s business as usual processes.
<p>Superannuation Prudential Guide 223: Fraud Risk Management [33] - [34].</p>	<p>The trustee should investigate all instances of actual or potential fraud that are detected. A robust fraud investigation seeks to determine facts and to identify risk issues and control weaknesses.</p> <p>These procedures would designate the person(s) responsible for overseeing and carrying out the investigation and establish rules relevant to the conduct of the investigation, such as rules governing the conduct of interviews, evidence handling, treatment of persons involved and reporting of outcomes.</p>
<p>Cross Prudential Standard 230: Operational Risk Management [13].</p>	<p>The Trustee should identify, assess, and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events; noting that operational risk is inherent in all products, activities, processes and systems.</p>

Detect	
<p>Cross Prudential Standard 230: Operational Risk Management [27].</p>	<p>The Trustee must maintain a comprehensive assessment of its operational risk profile. As part of this, the Trustee must:</p> <ul style="list-style-type: none"> a) Maintain appropriate and effective information systems to monitor operational risk, compile and analyse operational risk data and facilitate reporting to the Board and senior management; and b) Identify and document the processes and resources needed to deliver critical operations, including people, technology, information, facilities and service providers, the interdependencies across them, and the associated risks, obligations, key data and controls.
<p>Cross Prudential Standard 230: Operational Risk Management [23].</p>	<p>The Trustee must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.</p>
<p>ASIC Regulatory Guide 277 Consumer Remediation RG277.31.</p>	<p>The Trustee must maintain adequate systems and processes to identify misconduct or other failures that have or may have led to consumer loss.</p>
<p>Regulatory Guide 277: Consumer Remediation [47][a] – [e].</p>	<p>The Trustee should use data, complaints, trend analysis and known risk indicators to investigate how far the misconduct or other failure extends and understand which consumers are affected. The Trustee should specifically assess:</p> <ul style="list-style-type: none"> a) Whether other products, brands, advice or services might be involved; b) Whether systems, processes or policies might have failed; c) Whether representatives or employees might be implicated; d) Whether platforms or sales channels may be affected; or e) Whether business groups, product or service providers, subsidiaries or licensees might be impacted.

Report	
<p>Superannuation Prudential Guide 223: Fraud Risk Management [24][b].</p>	<p>The Trustee should give active consideration to past fraud incidents, both internal and external, including how the Trustee managed and resolved the incidents.</p> <p>In considering past fraud incidents, the Trustee should consider external sources of information that provide insight into broader market instances of fraud, in order to more fully understand the fraud risk environment.</p>
<p>Superannuation Prudential Guide 223: Fraud Risk Management [38].</p>	<p>The Trustee should operate a register to capture all incidents of detected fraud, to be analysed to further improve the Trustee's fraud risk management framework.</p>
<p>Superannuation Prudential Guide 223: Fraud Risk Management [43] [a] – [b].</p>	<p>The Trustee must maintain effective monitoring and review of the fraud risk management framework, including through:</p> <ul style="list-style-type: none"> a) Testing and review of the implementation and functioning of the fraud control plan. Prudent practice suggests that testing and review would be conducted by each of the Trustee's business units and the risk management function, through risk-based testing of controls that are considered to be most critical for the prevention of fraud or that may have previously failed to prevent or detect an incidence of fraud; and b) Independent evaluation of fraud risk controls by internal audit, to identify any control weaknesses and ensure corrective actions in response to past control weaknesses are effective.

Report	
Cross Prudential Standard 230: Operational Risk Management [16].	The Trustee must maintain appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events.
Cross Prudential Standard 234: Information Security [36].	The Trustee must notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.
Cross Prudential Standard 234: Information Security [35][a] – [b].	<p>The Trustee must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that:</p> <ul style="list-style-type: none"> a) Materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or b) Has been notified to other regulators, either in Australia or other jurisdictions.
Regulatory Guide 277: Consumer Remediation [46].	The Trustee must ensure that the full extent of any misconduct or other failure has been investigated, to identify how many consumers have been affected. There might be a question about whether the misconduct or other failure is more widespread than what initial evidence suggests.
Protecting Australians Against Scams and Fraud ASIC Letter to RSE Trustees 29 January 2025.	The Trustee must capture and record scam attempts accurately, so they have the necessary data to properly assess the real risk of scams to members. This observation is similarly applicable to fraud.

Report	
<p>Regulatory Guide 271: Internal Dispute Resolution [179] – [180].</p>	<p>The Trustee must record all complaints received and maintain an effective system for recording information about complaints. The system must allow for keeping track of the progress of each complaint.</p> <p>Trustees should design their complaints system to suit the nature, scale and complexity of their operations, including the number of complaints they receive. Use specialised complaints software or integrate complaint management data fields into existing customer relationship management systems.</p>

Disrupt	
<p>Competition and Consumer Act 2010 (Cth) s 58BX(1)(b) and 58BZA(2)(c) – (d).</p>	<p>Where actionable scam intelligence is held, the Trustee must take reasonable and proportionate actions to:</p> <ul style="list-style-type: none"> a) Disrupt the activity; or b) Prevent loss or harm, or further loss or harm³. <p>The Trustee must take this action within the earlier of:</p> <ul style="list-style-type: none"> a) 28 days; or b) The point at which the entity reasonably believes that the activity is or is not a scam.
<p>Competition and Consumer Act 2010 (Cth) s 58BY(2).</p>	<p>The Trustee must report actionable scam intelligence to the regulator within the period prescribed by the SPF rules; beginning on the earlier of:</p> <ul style="list-style-type: none"> a) 28 days after the actionable scam intelligence is acquired; or b) The day on which it is determined that the scam intelligence is or is not a scam.

³ Reasonable steps will be given clearer meaning through SPF Rules and SPF Code(s). See Competition and Consumer Law Act 2010 (Cth) s 58BB and 58BZ.

Disrupt	
Regulatory Guide 277: Consumer Remediation [304].	The Trustee should ensure that key decisions about scoping and remedies that will affect consumer outcomes should be evidence based and appropriately justified in the circumstances. Monitoring the remediation, specifically the consumer outcomes, will help improve this and future remediations. Learning and adapting to new information as it becomes available will help the Trustee achieve good consumer outcomes.

Respond	
Competition and Consumer Act 2010 (Cth) s 58BZ(1).	The Trustee must maintain a mechanism through which members and prospective members can report an activity that is or may be a scam related to, connected with, or which uses the Trustee's services.
Competition and Consumer Act 2010 (Cth) s 58BZD(1)(a).	The Trustee must develop and maintain an accessible and transparent IDR mechanism to deal with complaints about an activity that is or may be a scam related to, connected with, or which uses the Trustee's service.
Competition and Consumer Act 2010 (Cth) s58BZDA(1) – (2).	During scam-related IDR, the Trustee must provide a statement of compliance to the complainant that details whether the regulated entity is, based on information reasonably available to the entity at the time of making the statement, compliant with its obligations under the SPF provisions that are relevant to the complaint.
Competition and Consumer Act 2010 (Cth) s58BZF(1).	The Trustee must ensure that information about the rights of consumers to access: <ul style="list-style-type: none"> a) The scam reporting mechanism; and b) The IDR mechanism; and c) An External Dispute Resolution (EDR) scheme Is publicly accessible.

Respond	
Superannuation Prudential Guide 223: Fraud Risk Management [40].	The Trustee should develop a sound communication strategy addressing internal and external communication needs, including interaction with law enforcement agencies and regulators, and outlines procedures for responding to external enquiries that arise after fraud is detected.
Cross Prudential Standard 230: Operational Risk Management [16].	The Trustee must develop business continuity plan(s) (BCPs) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with severe but plausible scenarios.
Cross Prudential Standard 234: Information Security [24].	The Trustee must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).
Regulatory Guide 277 Consumer Remediation [42].	The Trustee must take all reasonable steps to access and secure the evidence, data and records held by the business or relevant external third parties that are necessary in order to complete remediation. This process should occur as early as possible in the remediation process to avoid any accidental or automatic erasure of evidence.
Regulatory Guide 277 Consumer Remediation [66].	To determine an appropriate remedy, the Trustee should assess available records to identify 'features' of affected consumers (or cohorts of consumers) that may be relevant to how misconduct or other failure may have affected them. For example, consumer cohorts who are suffering financial hardship or difficulty because of the misconduct or other failure, or have been identified as potentially experiencing vulnerability, may need additional remedies such as support services or professional assistance.

Respond	
<p>Regulatory Guide 277: Consumer Remediation [91].</p>	<p>In cases of misconduct or other failure, the Trustee should consider the affected consumer or cohorts of consumers' circumstances in determining what other non-monetary remedies or outcomes may be appropriate. For example:</p> <ul style="list-style-type: none"> a) providing legal or other assistance b) postponing or ceasing action c) pausing or waiving statutory limitation periods
<p>Regulatory Guide 277: Consumer Remediation [146].</p>	<p>In cases of misconduct or other failure, the Trustee should consider developing a communications plan that seeks to ensure affected consumers:</p> <ul style="list-style-type: none"> a) Understand what has happened; b) Are provided with updates when necessary and appropriate; c) Understand the remediation outcome and what it means for them, including how they can make further inquiries; d) Are able to easily follow any necessary calls to action, with support when needed; and e) Are told how they can make a complaint about the remediation outcome.
<p>Regulatory Guide 271: Internal Dispute Resolution [111].</p>	<p>The Trustee should establish appropriate links between their IDR process and AFCA. A complaint may go through the IDR process but remain unresolved, or may not be resolved within the relevant maximum IDR timeframe. The Trustee should:</p> <ul style="list-style-type: none"> a) Inform the complainant that they have a right to pursue their complaint with AFCA; and b) Provide details about how to access AFCA.

Respond	
Regulatory Guide 271: Internal Dispute Resolution [114].	<p>The Trustee should consider developing broader communications to consumers about their arrangements for managing complaints—including the publicly available complaint management policy, brochures explaining how to complain, relevant website frequently asked questions (FAQs) and call centre scripting should also effectively inform complainants of:</p> <ul style="list-style-type: none"> a) Their right to take their complaint to AFCA if they are dissatisfied; and b) The contact details of AFCA.
Regulatory Guide 271: Internal Dispute Resolution [134].	The Trustee’s IDR process must be easy to understand and use, including by people with disability or language difficulties.
Regulatory Guide 271: Internal Dispute Resolution [136].	The Trustee’s IDR process should be flexible about how complaints are lodged and offer multiple lodgement methods—including telephone, email, letter, social media, in person, or online. Complaints do not need to be in writing—in some cases, insisting that complaints are in written form can be a disincentive to the complainant.
Regulatory Guide 271: Internal Dispute Resolution [151].	The Trustee must provide complaint management staff with adequate materials and equipment to handle complaints. This includes scripts, FAQs, checklists, sample letters and templates, specialist support materials, complaint management IT systems and finances.
Regulatory Guide 271: Internal Dispute Resolution [79].	The Trustee should note that superannuation trustee complaints, except for complaints about death benefit distributions, must be responded to no later than 45 calendar days after receiving the complaint.



ASFA Scams Prevention Policy
Template