

ASFA Scams & Fraud Toolkit



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	5
2. Obligations map	10
3. Snapshot: Legislation relevant to Australian superannuation funds	12
4. Prevention, detection and response	15
5. Common superannuation fraud risks	18
6. Toolkit: Summary of advised outcomes in fraud and scam preparedness	20
7. Toolkit: Summary of indicative reporting timeframes	21
8. Fraud controls for superannuation	22
9. Snapshot: Sources of obligations	24
10. Additional resources	27



CEO Foreword

Mary Delahunty

The superannuation system is entrusted with something profound: the financial security of millions of Australians for their retirement.

With that responsibility comes a duty to protect those savings from fraud and scams, threats that grow more complex every day. Meeting this challenge is not the work of any one organisation alone. It requires the commitment of trustees, service providers, regulators, and policymakers working together to safeguard trust in the system and protect members' futures.

Fraud and scams are not new, but their scale and sophistication continue to grow. For many Australians, superannuation is their single largest financial asset outside the family home. Protecting it is a responsibility that cannot be taken lightly. Our controls must be strong, our vigilance constant, and our responses swift.

ASFA is committed to supporting the sector with the clarity and practical tools needed to meet this challenge. The ASFA Financial Crimes Protection Initiative (FCPI) was established to build the sector's collective capability to prevent, detect, and respond to financial crimes. Industry-led and collaborative, the FCPI unites funds and service providers to strengthen governance, controls, and resilience. This Fraud and Scams Toolkit is a product of that work – bringing together legislative and prudential obligations alongside better practice and member insights, so trustees have a clear and practical resource to guide them.

Our role is to support a superannuation system that Australians can rely on – not only for performance, but for protection. That responsibility is shared across the system, and it is one we must all uphold with diligence and care. The work outlined here is about preserving trust because a trusted superannuation system is good for every Australian – today, tomorrow, and into retirement.

Thank you for your continued commitment to safeguarding the security and sustainability of Australia's superannuation system.

Mary Delahunty
ASFA CEO

Introduction

The Association of Superannuation Funds of Australia (ASFA) is the voice of superannuation. Operating since 1962, we represent over 100 organisations, including corporate, industry, retail, and public sector funds, as well as critical service providers. ASFA unites the superannuation community, supporting our members with research, advocacy, education and collaboration to help Australians enjoy a dignified retirement. We promote effective practice and advocate for efficiency, sustainability and trust in our world-class retirement income system.

ASFA proudly represents 90 per cent of all 18 million Australians with superannuation. With over \$4 trillion in retirement savings under management, the superannuation system carries a significant responsibility, one that must be matched by strong regulatory compliance and operational resilience.

ASFA has made multiple submissions to government consultations on Australia's approach to Fraud and Scams, including with respect to the Government's Scams Prevention Framework Bill 2025.

Superannuation is the cornerstone of financial security for most Australians. ASFA will continue to advocate for strong safeguards for Australians superannuation, knowing that a trusted superannuation system is good for all Australians.

This toolkit brings together key legal obligations and prudential expectations that apply to superannuation trustees in relation to fraud and scams.

It draws on relevant legislation and guidance to help superannuation trustees, and their customers understand their legal obligations relating to the prevention and response of Scams and Fraud.

Together, these frameworks set out the regulatory expectations for trustees in protecting member data and maintaining operational integrity. This toolkit is intended to simplify, aggregate and explain existing laws and guidance and act as a practical resource for trustees and service providers.

It is designed to consolidate the regulatory requirements that apply to cyber resilience in the superannuation sector, and to assist users in interpreting and applying them in day-to-day operations.

It does not constitute legal advice, should not be relied upon as such, and superannuation fund trustees should seek their own independent advice regarding their rights and obligations.

About the contributors



Mark Bland

Partner | Financial Services

Mark provides advisory and transactional services to financial institutions, including superannuation trustees, fund managers, financial advisers, and license holders. He specialises in regulatory affairs, compliance advice, and responses to enforcement actions. His expertise covers AFS and RSE licensee obligations, applications, conduct, and disclosure as well as privacy and AML/CTF laws.



Sebastian Reinehr

Policy Director | ASFA

Sebastian Reinehr is Policy Director at ASFA. He has extensive policy expertise related to combatting cybersecurity threats and financial crime. He previously served as Policy Director at the Australian Finance Industry Association and as an Adviser and Senior Adviser to the Opposition Leader and senior Cabinet and Shadow Cabinet Ministers.



Relevant legislation

The Commonwealth legislation drawn upon in creation of this Toolkit includes the following:

1. *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
2. *Autonomous Sanctions Act 2011*
3. *Autonomous Sanctions Regulations 2011*
4. *Competition and Consumer Act 2010*
5. *Corporations Act 2001*
6. *Financial Accountability Regime Act 2023 and associated rules*
7. *Superannuation Industry (Supervision) Act 1993*
8. *Privacy Act 1988*
9. Prudential Standard CPS 230 Operational Risk Management
10. Prudential Standard SPS 220 Risk Management
11. Prudential Standard SPS 114 Operational Risk Financial Requirements
12. Prudential Standard SPS 510 Governance
13. Prudential Practice Guide SPG 223 Fraud Risk Management
14. Prudential Practice Guide CPG 230 Operational Risk Management
15. Prudential Practice Guide SPG 220 Risk Management

The toolkit is designed to simplify, aggregate and explain the relevant laws and guidance. It is not legal advice and should not be relied upon as such. Superannuation funds and their service providers should obtain independent advice in relation to their specific obligations.

ASFA acknowledges the contribution of Mills Oakley, whose support and legal expertise in reviewing the content of this toolkit has helped ensure its accuracy and relevance.

ASFA provides this resource to support stronger compliance and promote a consistent approach to cyber resilience across the superannuation sector.



About this Toolkit

The risk of scams and fraud poses significant security challenges for the broader Australian economy including trustees of superannuation funds and their service providers. Of the 11,000 instances of scams complaints received by the Australian Financial Complaints Authority (AFCA) there were fewer than 20 superannuation-related transactions. Nonetheless, superannuation trustees should still be vigilant for scams and fraudulent activity.

Scams and fraudulent activity continue to pose a significant and growing threat to individuals, businesses, and the Australian economy. In response, the Australian Government has taken a number of steps to strengthen national resilience against the threat of scams and fraudulent activity. These steps include amending the *Competition and Consumer Act 2010* to introduce the Scams Prevention Framework, which provides clear guidance for industry to enhance scam prevention, detection, and response mechanisms.

While the Scams Prevention Framework does not currently apply to superannuation funds, it is nonetheless something that trustees should consider in developing their approaches to these issues.

In addition, the National Anti-Scam Centre (NASC) has been established by the Australian Competition and Consumer Commission (ACCC) which facilitates real-time information sharing, operational coordination, and collaborative disruption of scam operations across sectors.

Together, these initiatives form part of a broader policy and legislative agenda aimed at reducing the impact of scams and fraud, including the provision of guidance to industry.

Key legislative obligations under the *Superannuation Industry (Supervision) Act 1993*, the *Financial Accountability Regime Act*, and the *Corporations Act 2001* (*Corporations Act*), require businesses to prepare for, report, and respond to scams and fraudulent activity.

Trustees also have relevant obligations under prudential standards, including:

1. Prudential Standard SPS 220 Risk Management;
2. Prudential Standard 114 Operational Risk Financial Requirements;
3. Prudential Standard 510 Governance and CPS 230 Operational Risk Management; (which replaces SPS 231 Outsourcing); and
4. SPS 232 Business Continuity Management on 1 July 2025.

Role of the Board and Senior Management

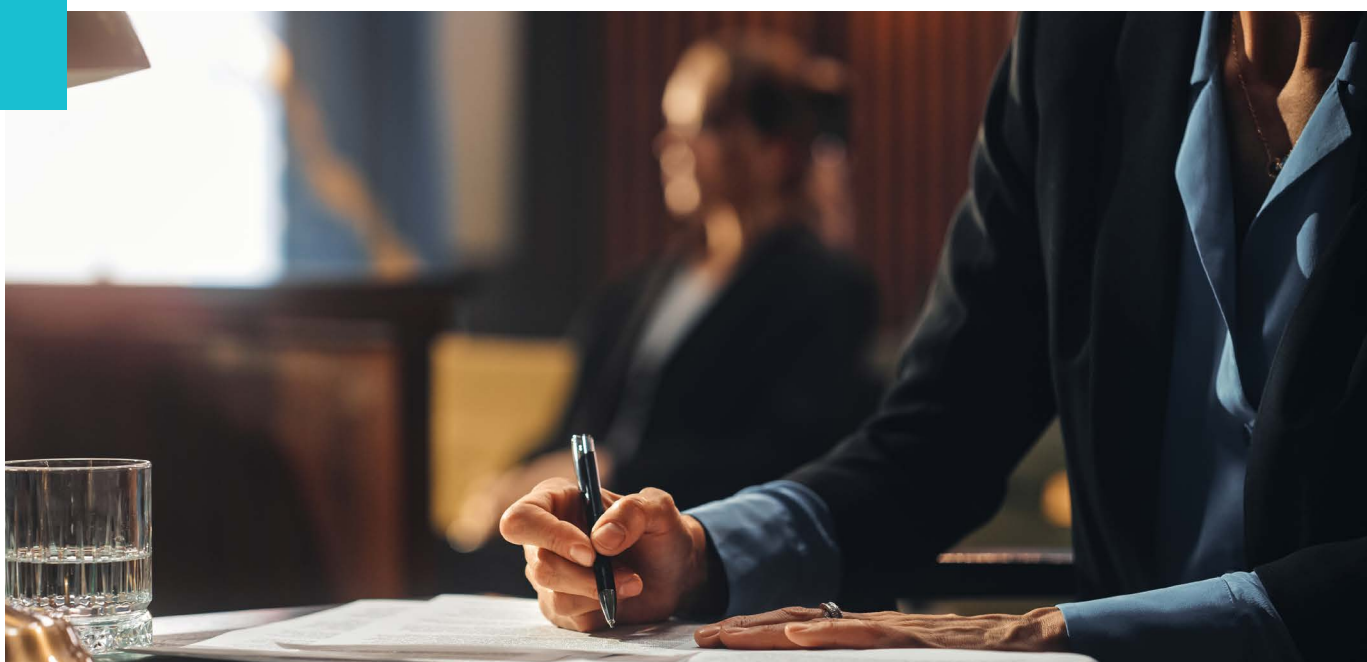
Under SPS 220 Risk Management, trustees are responsible for ensuring that their risk management framework covers all material risks to its business operations, including fraud risk, which APRA consider is a subset of operational risk.

The Board of a superannuation trustee is ultimately responsible for the risk management framework for the trustee. The Board is therefore responsible for ensuring that the risk management framework adequately addresses fraud risk.

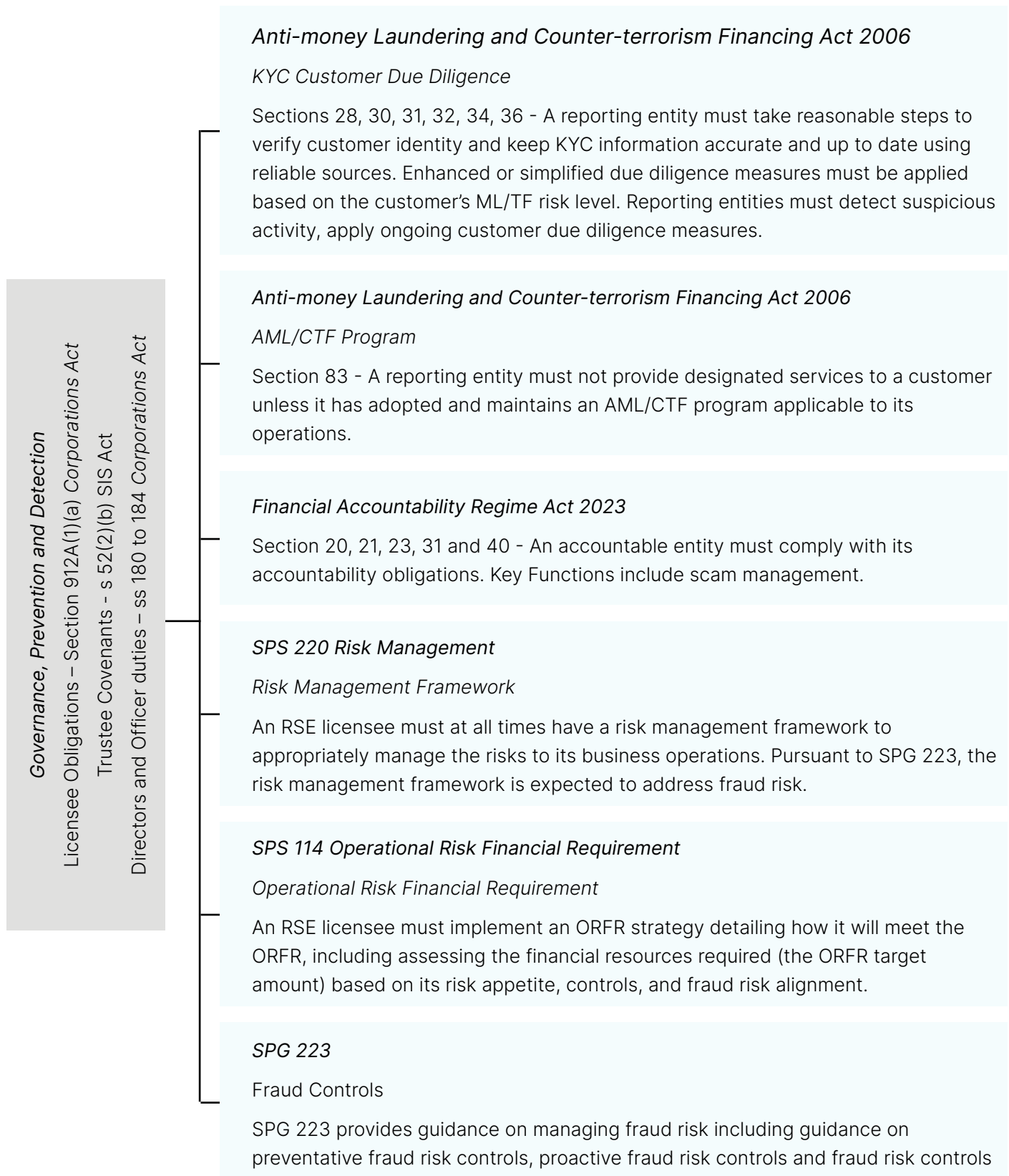
For the purposes of the Operational Risk Financial Requirement under Prudential Standard SPS 114 Operational Risk Financial Requirement, an RSE licensee must determine the financial resources necessary to address operational risks that it has identified in its risk management framework, taking into account its risk appetite and appropriate risk mitigations and controls (the ORFR target amount).

SPG 223 Fraud Risk Management sets out that a core element of an effective risk management framework is a strong risk culture that exhibits organisational attributes and behaviours which reflect an intolerance of fraud. A risk management framework should address fraud risk.

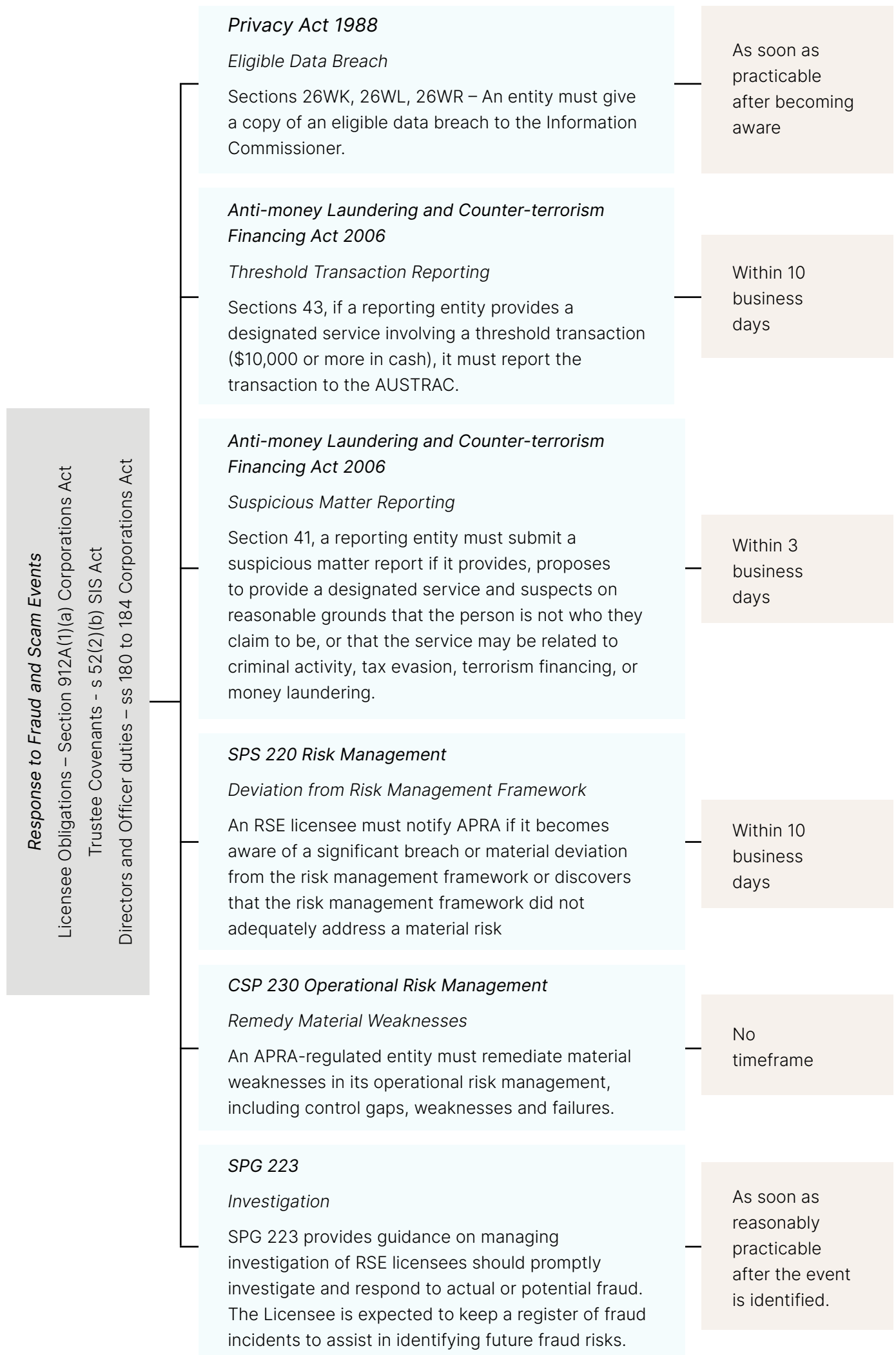
APRA expects that a prudent RSE licensee will develop a suite of fraud risk controls related to the prevention, detection and response to fraudulent activity.



Obligations map



*Amendments to the Anti-money Laundering and Counter-terrorism Financing Act 2006 including customer due diligence are coming into effect on 31 March 2026.



Snapshot: Legislation relevant to Australian superannuation funds

RSE licensees may wish to consider the following laws to ensure their risk management framework adequately addresses the risk of scams and fraud:

Privacy Act 1988 (Privacy Act)	
Applicability	Australian Government agencies and organisations with an annual turnover of more than \$3 million or with an Australian Financial Services (AFS) licence. Certain other entities may be subject to requirements depending on business operations.
Summary	The Privacy Act regulates how personal information is handled by Australian Government agencies and organisations with an annual turnover of more than \$3 million and all AFS licensees. It includes 13 Australian Privacy Principles that set standards for the collection, use, storage, and disclosure of personal information. Ensuring compliance with the Privacy Act requires implementation of robust data protection measures and provides for reporting obligations detailed in the Notifiable Data Breach Scheme.
Administering Body	Office of the Australian Information Commissioner
More Information	Privacy Act OAIC
Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)	
Applicability	Applies to reporting entities that provide designated services, which includes RSE licensees when they accept superannuation contributions, rollovers or transfers related to a member, or when they pay out a member's interest.
Summary	The AML/CTF Act adopts a risk-based approach to AML/CTF compliance, under which Reporting Entities are required to comply with obligations that fall under the following categories: • Identification and verification: REs must (subject to exemptions for superannuation trustees relating to contributions and rollovers (s 39 AML/CTF Act); and cashing of low value balances and Departing Australia Superannuation Payments; risk only life policy interests in a superannuation fund (Chapter 41 AML/CTF Rules) verify a customer's identity before providing designated services and conduct ongoing due diligence. • Reporting: REs must report suspicious matters, certain transactions above specified thresholds, and international funds transfer instructions to AUSTRAC. • AML/CTF Program: REs must develop, maintain, and comply with an AML/CTF program to identify, manage, and mitigate the risks of money laundering and terrorism financing. Members of a Designated Business Group (DBG) may share a joint program. • Record keeping: REs are required to retain specified records, including those provided by customers, for at least seven years. A number of amended obligations under the AML/CTF Act are scheduled to come into effect at the end of March 2026.
Administering Body	Australian Transaction Reports and Analysis Centre
More Information	AML/CTF Act AUSTRAC
Autonomous Sanctions Act 2011	
Applicability	Applies to all individuals and body corporates including RSE licensees.
Summary	The Autonomous Sanctions Act 2011 provides the Minister an ability to determine certain designate a person or entity for the purpose of applying sanctions (such as asset freezes or travel bans), provided the designation meets the criteria set out in the Autonomous Sanctions Regulations 2011. The Autonomous Sanctions Regulations 2011 outline the specific types of sanctions that can be imposed—such as travel bans, asset freezes, and restrictions on trade or services.
Administering Body	Department of Foreign Affairs and Trade
More Information	Australia and sanctions DFAT



Corporations Act 2001	
Applicability	Australian Financial Services (AFS) licensees and Australian credit licensees.
Summary	The Corporations Act provides a uniform framework for company formation, governance, and insolvency in Australia. It regulates company responsibilities, including shareholder rights and directors' duties, ensuring transparency and accountability in corporate activities. It also contains obligations relating to the provision of financial services, including providing a superannuation trustee service. Protections against scams and fraud are likely to be relevant to a licensee's obligation to ensure that financial services are provided "efficiently, honestly and fairly". The Corporations Act sets requirements for entities providing financial services to submit notifications about 'reportable situations' (which may include among other matters significant data breaches) to the Australian Securities and Investments Commission.
Administering Body	Australian Securities and Investments Commission
More Information	Reportable situations ASIC
Superannuation Industry (Supervision) Act 1993 (SIS Act)	
Applicability	Regulated superannuation funds, approved deposit funds, and pooled superannuation trusts
Summary	The SIS Act establishes the regulatory framework for superannuation funds in Australia to ensure they are operating prudently and in members' best financial interests. It applies to trustees of regulated superannuation entities that have elected to be regulated and are supervised by either APRA (for most large funds) or the ATO (for SMSFs). The SIS Act includes trustee and director covenants, including the requirements to exercise care, skill and diligence and to have robust risk management frameworks. It provides enforcement powers and penalties for non-compliance.
Administering Body	Australian Prudential Regulation Authority
More Information	Legislation for Superannuation Entities APRA
Financial Accountability Regime Act 2023 (FAR Act)	
Applicability	Accountable entities including RSE licensees
Summary	The FAR Act establishes a framework requiring accountable entities to follow several broad obligations including to conduct its business with honesty and integrity, and with due skill, care and diligence. Accountable entities are required to appoint and register accountable persons that collectively cover all areas of the business operations of the accountable entity and its relevant group. The regulator rules prescribe certain key functions for inclusion in the FAR register. Key functions are functional areas that are deemed to be of particular importance from a prudential and conduct perspective. Key functions most relevant to scams and fraud are risk management, data management, operational risk, scam and technology management, and staff training.

Prudential Standard SPS 114 — Operational Risk Financial Requirement (SPS114)	
Applicability	RSE Licensees
Summary	SPS 114 requires an RSE licensee to maintain, manage and utilise, in accordance with this prudential standard, financial resources to protect beneficiaries from losses due to operational risk that relates to the RSEs within its business operations. Key requirements include having a documented ORFR strategy, an ORFR target amount and tolerance limit. It also sets obligations for RSE Licensees to maintain adequate financial resources to address losses arising from operational risks. From 1 July 2025, the ORFR can also be used to ensure the effective management and prevention of operational risk incidents, including the remediation of identified material weaknesses and maintenance of critical operations within tolerance levels through severe disruption.
Administering Body	Australian Prudential Regulation Authority
More Information	CPS 234 Information Security Prudential Handbook APRA
Prudential Standard CPS 230 —Operational Risk Management (CPS230)	
Applicability	APRA-regulated entities.
Summary	CPS 230 requires APRA-regulated entities to identify, assess, and manage operational risks through robust internal controls, continuous monitoring, and remediation. The standard also requires entities to manage risks associated with service providers by implementing a comprehensive service provider management policy, establishing formal agreements, and conducting rigorous oversight.
Administering Body	Australian Prudential Regulation Authority
More Information	CPS 230 Operational Risk Management Prudential Handbook APRA
Prudential Standard SPS 220—Risk Management (SPS220)	
Applicability	APRA-regulated entities.
Summary	SPS 220 establishes requirements for APRA-regulated entities to maintain a risk management framework that covers all material risks. SPG 223 specifically states that APRA expects a Risk Management Framework to address Fraud Risk including internal and external fraud risk. The framework must be consistent with the entity's strategic objectives and business plan. It sets obligations for Boards of regulated entities to approve a risk management strategy, business plan and risk appetite statement as part of a risk management framework that is appropriate to the size, business mix and complexity of the entity. SPG 223 sets out APRA's expectation that an RSE licensee would consider the adequacy of resources to support its fraud risk management framework as part of this process. It also sets obligations for regulated entities to notify APRA when they become aware of a significant breach of, or material deviation from, the risk management framework, or that the risk management framework does not adequately address a material risk, including material information security and cyber security risks.
Administering Body	Australian Prudential Regulation Authority
More Information	SPS 220 Risk Management Prudential Handbook APRA

Prevention, Detection & Response

What is a “fraud” and a “scam”?

APRA states in SPG 223 what it considers to be fraud: The Cyber Act gives us the legislated definition of a cyber security incident as being:

- **Internal Fraud** - losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy (excluding diversity/discrimination events) which involves at least one internal party; and
- **External Fraud** - losses due to acts of a third party that are of a type intended to defraud, misappropriate property or circumvent the law.

Scam is a narrower concept than “fraud”. It is defined by the Australian Government’s National Anti-Scam Centre as when someone deceives a person to steal their money or personal information.

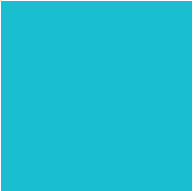
ASIC Report 761: Scam prevention, detection and response by the four major banks defined scams as a type of fraud, usually with the purpose of getting money or information from people using a deceptive scheme or trick.

Governance of Fraud and Scam Risks

Under APRA’s prudential standards, an RSE licensee is required to develop and maintain a range of documents addressing fraud prevention as part of its broader risk management obligations.

SPS 220 Risk Management and SPG 223.6 requires a trustee to establish a Fraud Risk Management Framework that is integrated into its overall Risk Management Framework. It must also develop a Risk Appetite Statement as outlined in SPG 223.7, which articulates its intolerance for fraud risks while recognising that such risks cannot be fully eliminated.

Pursuant to SPG 223.8, the fraud risk management approach must be effectively communicated both internally and externally to ensure broad awareness and understanding. Under *SPS 114 Operational Risk Financial Requirement* and SPG



223.10, the trustee is also required to assess and document the financial resources needed to address losses arising from fraud and other operational risks, ensuring consistency with its ORFR target amount.

As specified in SPG 223.12 and SPS 220 Risk Management, the role of the risk management function must include clear responsibilities for the oversight of fraud risk. The trustee must maintain adequate financial, human, and technical resources to support its risk management framework, including fraud risk management.

Detection of Fraud and Scam Risks

Under APRA's *Prudential Practice Guide SPG 223 Fraud Risk Management*, trustees are expected to implement comprehensive fraud detection measures as part of their risk management framework. These measures encompass both proactive and reactive controls to identify and mitigate fraud risks effectively:

- **Proactive fraud detection controls** involve systematic monitoring of financial and operational data to identify anomalies indicative of fraudulent activity such as suspicious trends. Trustees should consider engaging internal or external auditors to enhance fraud risk controls.
- **Reactive fraud detection controls** are designed to detect fraud after it has occurred. These include assessing discrepancies in reconciliations, verifying asset records and values, monitoring transactions for unauthorized activity, implementing whistleblowing policies, and providing targeted training to staff responsible for managing fraud risk controls.

Trustees are expected to maintain a fraud incident register documenting all fraud incidents.

Responding to Fraud and Scam Events

APRA expects trustees to have clear and effective procedures in place for responding to actual or suspected fraud. Prompt investigation is essential to minimise losses and mitigate broader risk exposures, with investigations aimed at establishing the facts, identifying risks, and addressing any control weaknesses. Investigations should be undertaken by skilled and personnel independent to the relevant business unit, which may include senior managers or external consultants.

Trustees are expected to have a formal referral process to determine whether the incident should be reported to law enforcement or whether a Significant Event Notice should be lodged with APRA. Pursuant to CPS 230, trustees must remediate material weaknesses in their operational risk management framework in a timely manner. Other time-based response requirements are detailed in Section 6.



Scams Prevention Framework – a new model

The Scams Prevention Framework Act 2024 amended the Competition and Consumer Act 2010 to introduce a regulatory regime designed to strengthen the obligations of regulated entities in preventing, detecting, and responding to scam activity associated with their services.

The Scams Prevention Framework (SPF) does not currently apply to trustees, although it is likely to apply to trustees in the future. Therefore, trustees should consider aligning their practices with the SPF where possible.

Regulated entities must establish *SPF Policies* that document and implement robust governance policies and procedures for the prevention, detection, disruption, and response to scams.

The SPF has detailed response obligations. For example:

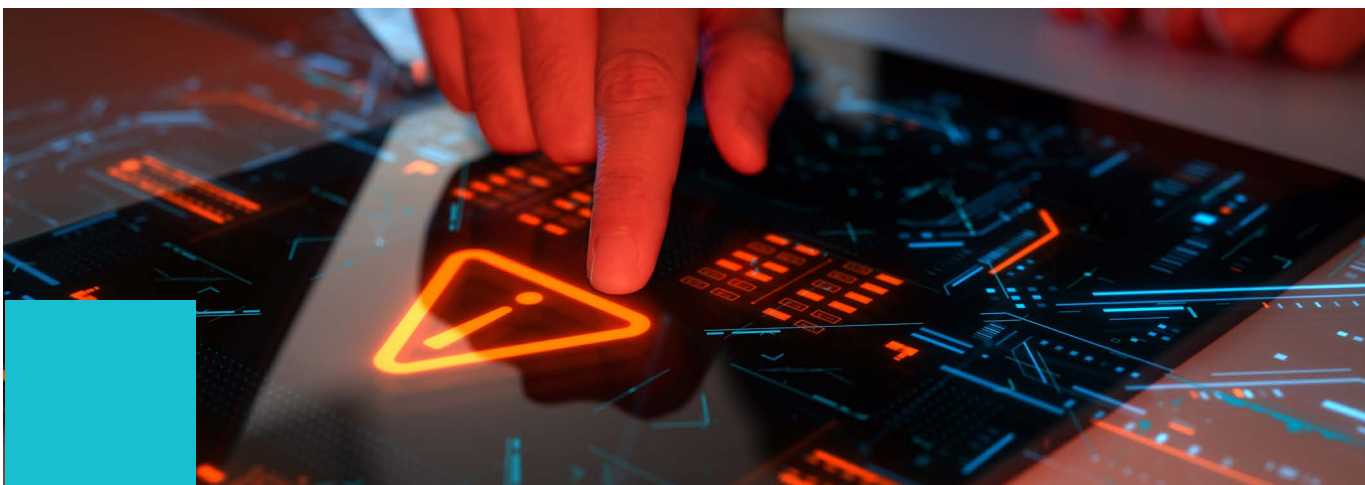
- entities holding actionable scam intelligence must report it within 28 days and take reasonable steps, in a timely manner, to identify affected individuals who were SPF consumers at the relevant time;
- entities must act to disrupt scam activity or prevent resulting loss or harm when in possession of such intelligence;
- entities are also required to have an accessible reporting mechanism for individuals to flag suspected scams associated with their services, as well as a transparent and accessible internal dispute resolution process to manage complaints about scams; and
- entities must publish clear information on SPF consumers' rights in relation to scam reporting, the internal dispute resolution mechanism, and, if applicable, the external dispute resolution scheme.

Common Superannuation Fraud Risk

While each trustee faces unique operational environments and risk profiles, it is essential that they remain acutely aware of their own specific fraud vulnerabilities.

However, both APRA and ASIC have identified a range of common fraud risks affecting the broader superannuation sector. These include:

1. **Unauthorised Transfer:** transferring funds out of their superannuation account to a scammer (for example when a pension is established and payments are made to a scammer's bank account).
2. **Rollover Fraud:** rolling over from an APRA regulated fund to a self-managed superannuation fund where the bank account is actually a scammer's staging account.
3. **Personal Information Scam:** aiding a scammer to make a transfer by disclosing personal information.
4. **Member Identify Fraud:** fraudulent use of a member's identity to gain unauthorised access to superannuation benefits.
5. **Process Manipulation:** manipulation or misuse of accounts payable processes.
6. **Misuse of Confidential Information:** misuse of confidential or commercially sensitive information to benefit a member, employee, or outsourced service provider.
7. **Access to Trustee Systems:** unauthorised access to information systems leading to theft of data and/or fraud.



Controls for common types of fraud risk

To effectively mitigate fraud risk in the superannuation sector, robust and tailored controls should be in place for all transaction types. For electronic transactions, multi-factor authentication (MFA) should be a standard requirement to ensure the integrity of member interactions and prevent unauthorised access.

For transactions initiated in person or via paper-based channels, certified identification should be obtained alongside other independent verification methods such as recent transaction history, account balances, or knowledge-based authentication questions.

Additional procedures should be applied to transactions deemed higher risk or high impact, such as direct member contact to confirm authenticity of the transactions. All fraud prevention measures should be inclusive and sensitive to the diverse needs of members, including those with low digital capability, disabilities, limited English proficiency, those experiencing financial hardship, or those affected by domestic or family violence.

More information on these controls can be found in Section 7.



Toolkit: Summary of advised outcomes in fraud and scams preparedness

Category	Advised Outcome	Key References	Specific Object Link
Governance & Oversight	Boards and executives should ensure their fund has implemented fraud risk into its Risk Management Framework and ORFR. If possible, the board should develop SPF Policies.	SPG 223 Fraud Risk Management	SPG 223 Fraud Risk Management para 6 to 14
		SPS220 Risk Management	SPS220 The Role of the Board Paras 5 to 8
		SPS 510 Governance	SPS 510 Role of the Board
		CPS 230 Operational Risk Management	CPS 230 Roles and responsibilities Paras 20 to 23 and Para 58
		Financial Accountability Regime Act 2023	Financial Accountability Regime Act 2023 Accountability obligations and Key Personnel obligations
Regulatory Notifications	Regulatory bodies such as APRA, OAIC, and ASIC are notified within relevant required reporting timeframes of any reportable incidents involving fraud risks or privacy breaches for Personal Information Scams.	SPS 220 Risk Management	SPS 220 Risk Management Para 37
		Privacy Act (NDB Scheme)	The Privacy Act 1988 Division 3
		RG104 AFS Licensing	RG104.29 Reporting on your Measures
		29JA of the Superannuation Industry (Supervision) Act 1993	APRA Notify a Breach
		CPS 230 Operational Risk Management	CPS 230 Notification Requirements Paras 33, 42 and 59
		Financial Accountability Regime Act 2023	Financial Accountability Regime Act 2023 Accountability obligations and Key Personnel obligations
Stakeholder Communication	Trustees should communicate with the relevant business unit and customer that may be affected by a fraud or scam event.	SPG 223 Fraud Risk Management	SPG 223 Fraud Risk Management para 6 to 14
		CPS 230 Operational Risk Management	CPS 230 Communications Strategy Para 40
Control Development	Develop to trolls to prevent and detect fraud and scams using both proactive and reactive methods ensuring ensure members' personal and financial data are safeguarded.	Privacy Act (as distinct from the NDB Scheme)	Federal Register of Legislation - The Privacy Act 1988
		SPG 223 Fraud Risk Management	SPG 223 Fraud Risk Management para 23 to 31
		SPS220 Risk Management	SPS220 Risk Management para 16
		ASIC Report 761: Scam prevention, detection and response by the four major banks	Report 761 Preventing Scams Pages 8 to 15
Investigation	Trustees should promptly investigate and respond to actual or potential fraud. Investigations should establish facts, identify risks, and address control weaknesses.	SPS220 Risk Management	SPS220 Risk Management Declaration Para 32
		CPS 230 Operational Risk Management	CPS 230 Root cause identification Para 31
		SPG 223 Fraud Risk Management	SPG 223 Fraud Risk Management para 32 to 35

Toolkit: Summary of indicative reporting timeframes

Source of Obligation	Obligation	Recipient	Timing	Relevant Tests & Assessments
Privacy Act	Notifiable Data Breach	OAIC	As soon as practicable*	• Application & Exemption • Credit Reporting, Credit • Providers & TFN Rule Tests • Impacted Information Type Assessments • Eligible Data Breach Test (inc. Serious Harm Test) * Entities must notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner (s 26WL(3)).
Corporations Act	Reportable Situations	ASIC	Within 30 days	• Application • Nature of the Situation or Investigation • Significance & Material Impact
CPS 230	Operational Risk Incident	APRA	Within 72 hours	• Material Financial Impact or material impact on the ability of the entity to maintain critical operations
CPS 230	Disruption to Critical Operation	APRA	Within 24 hours	• Disruption outside tolerance
CPS 230	Service Provider Agreement	APRA	Within 20 business days	• Entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation • Entering into or significantly changing any material offshoring arrangement
SPS 220	Deviation from Risk Management Framework	APRA	Within 10 business days	• Trustee aware of significant breach of the risk management framework • Trustee aware of material deviation from risk management framework • Risk management framework did not adequately address a material risk
AML/CTF Act	Suspicious Matter Report	AUSTRAC	Within 3 business days	• reporting entity commences to provide designated service • reporting entity suspects on reasonable grounds that the first person is not the person the first person claims to be • preparatory to the commission of financing of terrorism or money laundering
AML/CTF Act	Threshold Transaction	AUSTRAC	Within 10 business days	• reporting entity commences to provide designated service • provision of the service involves a threshold transaction

Fraud controls for superannuation

The tables below defines key events and relevant vulnerabilities in the superannuation account lifecycle from a fraud perspective, and proposed common minimum control requirements funds should deploy. It is acknowledged funds may also conduct other system-wide controls to detect fraud activity.

The key controls relate to the following transactions:

1. the creation of new web-based member-initiated accounts;
2. a change of contact details initiated directly by the member;
3. rollovers between APRA regulated funds;
4. rollover from APRA regulated fund to SMSF; and
5. withdrawal or pension commencement .

Account Lifecycle - account creation and change of details

Account Lifecycle	Creation of new web-based member-initiated account *Does not include employer accounts, accounts created through a financial adviser, or paper-based account creation by a member	Change of contact details initiated directly by a member *All accounts. Does not include change of account details by an authorised person (financial adviser) acting on member's behalf	SuperMatch request by a member All accounts
Event Description	A new account is opened in a fund by a member using an online account creation process.	Member information added for first time	Funds request a list of active information for a member from ATO.
Key risks / vulnerabilities	'Staging' account created using fraudulent details to: test fund processes, link to myGov, control a legitimate account and effect a rollover to a new fund. Can lead to increase in compromised myGov accounts including to access government benefits.	Increase in compromise of phone numbers, email addresses – fraudster accesses account and changes details to effect rollover or withdrawal.	Connect SuperMatch to newly opened fraudulent account. Discovery of existing accounts often followed by rollover of member funds into fraudulent account.
Current verification requirements	No Know Your Customer (KYC) requirement. Trustee assessment is risk based.	No KYC requirement. However, a Proof of Identity check (or account ownership check) is performed. Trustee assessment is risk-based.	KYC must be completed (electronic or document-based) to a prescribed level before the fund can activate a SuperMatch search.
Current fund controls	Not universal. Controls vary from collection of standard personal details through to requiring electronic ID verification, combined with other fund system-wide fraud monitoring and screening techniques.	Funds generally apply Multi-Factor Authentication (MFA) or similar method (e.g. member portal) to contact the member to verify these changes. However, the application of these techniques is not universal.	As per prescribed SuperMatch requirements.
Minimum requirement – ASFA Better practice (in addition to existing regulatory requirements)	KYC – electronic ID (using the Document Verification Service (DVS)) to verify member, or document-based verification.	Multi-Factor Authentication (MFA), push notification via SMS and/or email, and/ or a prompt to access member portal to authorise completion of transaction. Change of mobile phone number should require confirmation via the existing and new phone numbers.	As per prescribed SuperMatch requirements.

Account Lifecycle - consolidation, rollovers and paying benefits

Account Lifecycle	Consolidation and rollover between APRA funds All accounts	Consolidation and rollover from APRA fund to SMSF All accounts	Member requests a benefit paid or pension commenced All accounts
Event Description	Movement of money (part of full balance) from one fund to another or within a fund.	Movement of money (part of full balance) from an APRA fund to an SMSF.	Request to access balance through lump sum withdrawal, commencing a pension or early release.
Key risks / vulnerabilities	Unauthorised movement of member balances into fraudulent APRA fund account.	Rollover to SMSF using fraudulent identity which passes KYC protocols. Fraudulent bank account on SMSF used (unable to be detected).	Unauthorised movement of member balances out of system or to commence pension using fraudulent identity documentation.
Current verification requirements	KYC not required. Member must provide the transferring fund with: their name, address, date of birth and Tax File Number (TFN). Fund then checks the details match those on their system and validates the TFN with the ATO. Three-day rule – benefits required to be rolled over within the later of three business days of receiving the rollover request or the fund receiving all mandatory information (including any Suspicious Matter Reports (SMRs) requiring enhanced due diligence).	KYC must be completed – process is non-prescriptive and risk-based. 3 day rule – benefits required to be rolled over within the later of 3 business days of receiving the rollover request or the fund receiving all of the mandatory information (after KYC and bank check completed).	KYC must be completed – process is non-prescriptive and risk-based.
Current fund controls	Varies from SMS/email notifications to risk-based verifications deployed in certain instances if a system control flags a concern	KYC must be completed – process is non-prescriptive and risk-based. Funds use either electronic ID (using DVS) or document based. Additional controls may also be applied.	KYC must be completed – process is non-prescriptive and risk-based. Funds use either electronic ID (using DVS) or document based. Additional controls may also be applied.
Minimum requirement – ASFA Better practice (in addition to existing regulatory requirements)	Push notifications (SMS or email) to make member aware of request to rollover. Ideally a series of alerts at key stages of transaction. (Given the Three-day Rule, using MFA to authorise a rollover can currently act as a potential barrier and may not be preferred. Whilst a push notification does not provide complete assurance that the member responds to a fraudulent attempt within the timeframe in all cases, the centralised fraud register would bolster a funds ability to claw back funds where necessary).	Push notifications (SMS or email) to make member aware of request to rollover. Ideally a series of SMS alerts at key stages. OR Member authentication^ (completed on a risk-based approach and/ or based on materiality).	MFA, push notification via SMS or email, or prompt to access member portal to authorise completion of transaction. OR Member authentication^ (completed on a risk-based approach and/ or based on materiality). [It is not envisaged either of these requirements would be imposed with each regular partial withdrawal.]

Snapshot: Sources of Obligations

The obligations relating to an RSE licensee's incident response arise from multiple sources, including. Depending on the nature and scope of the incident, organisations may be required to report breaches to regulatory authorities, notify affected individuals and take remedial actions to prevent recurrence.

Privacy Act 1988

Type: Legislation | **Applicability:** Organisations with a turnover more than \$3 million | (*Privacy Act*)

Notifiable Data Breach Scheme

Under the Notifiable Data Breach Scheme any organisation or agency the *Privacy Act* covers must notify affected individuals and the Office of the Australian Information Commissioner when a data breach is likely to result in serious harm to an individual whose personal information is involved.

Source: Privacy Act – Part IIIC Division 3

Financial Accountability Regime Act 2023

Type: Legislation | **Applicability:** Accountable Entities including RSE Licensees | (*FAR Act*)

Appointment of Accountable Persons

An accountable entity must comply with its accountability obligations and appoint responsible persons that are responsible for Key Functions of the accountable entity. Key functions relevant for include scam management and training and monitoring of relevant staff.

Source: FAR Act – Chapter 2

Corporations Act 2001

Type: Legislation | **Applicability:** Australian Financial Services | (*Corporations Act*)

Reportable Situations

Australian financial service licensees are required to notify ASIC of all reportable situations.

Source: Corporations Act – Part 7.6 Division 3

Corporations Act 2001

Type: Legislation | **Applicability:** Australian Financial Services Licensee | (*Corporations Act*)

Licence Obligations

Australian Financial Service Licensees must act efficiently, honestly and fairly and (if an RSE licensee also acts as a responsible entity of a registered scheme) have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence.

Source: Corporations Act – Part 7.6 Division 1 – Sections 912A(1)(a), (d) and (h)

Corporations Act 2001

Type: Legislation | **Applicability:** Directors and officers of a corporation | (Corporations Act)

Directors' and Officers' Duties

Directors and Officers have duties to act with care and diligence, to act in good faith and in the best interests of the company, to avoid conflicts of interest, and to not improperly use their position or information to gain an advantage or cause harm.

Source: Corporations Act – Chapter 2D – Sections 180 to 184

Superannuation Industry (Supervision) Act 1991

Type: Legislation | **Applicability:** Corporate Trustee & Director of a Corporate Trustee | (SIS Act)

Trustee Covenants

A Trustee must exercise the same degree of care, skill and diligence as a prudent superannuation trustee would exercise.

Source: SIS Act – Part 6 – Section 52(2)(b) and 52A(2)(b)

Anti-money Laundering and Counter-terrorism Financing Act 2006

Type: Legislation | **Applicability:** Reporting Entity that provides a Designated Service | (AML/CTF Act)

Customer Due Diligence

A reporting entity must take reasonable steps to verify customer identity and keep KYC information accurate and up to date using reliable sources. Enhanced or simplified due diligence measures must be applied based on the customer's ML/TF risk level.

Source: AML/CTF Act – Part 2 – Sections 28 to 36

Anti-money Laundering and Counter-terrorism Financing Act 2006

Type: Legislation | **Applicability:** Reporting Entity that provides a Designated Service | (AML/CTF Act)

AML/CTF Program

A reporting entity must maintain an AML/CTF program applicable to its operations.

Source: AML/CTF Act – Part 7 – Sections 83

Anti-money Laundering and Counter-terrorism Financing Act 2006

Type: Legislation | **Applicability:** Reporting Entity that provides a Designated Service | (AML/CTF Act)

Reporting

A reporting entity must make threshold transaction and suspicious matter reports.

Source: AML/CTF Act – Part 3

Prudential Standard SPS 220

Type: Standard | **Applicability:** APRA-regulated entities | (SPS510)

Risk Management Framework

RSE licensees must at all times have a risk management framework to appropriately manage the risks to its business operations including fraud risk.

Source: SPS220 Risk Management – The role of the Board and senior management

Prudential Standard SPS 114

Type: Standard | **Applicability:** APRA-regulated entities | (SPS510)

Operational Risk Financial Requirement

An RSE licensee must implement an ORFR strategy detailing how it will meet the ORFR, including assessing the financial resources required to address fraud risk.

Source: SPS 114 Operational Risk Financial Requirement

Prudential Standard SPS 220

Type: Standard | **Applicability:** APRA-regulated entities | (SPS510)

Risk Management Framework

RSE licensees must at all times have a risk management framework to appropriately manage the risks to its business operations including fraud risk.

Source: SPS220 Risk Management – The role of the Board and senior management

Prudential Standard SPS 114

Type: Standard | **Applicability:** APRA-regulated entities | (SPS510)

Operational Risk Financial Requirement

An RSE licensee must implement an ORFR strategy detailing how it will meet the ORFR, including assessing the financial resources required to address fraud risk.

Source: SPS 114 Operational Risk Financial Requirement



Additional Resources

ASIC – Scams – This page contains information and alerts about scammers impersonating ASIC, scams-related information and resources, and a form to notify ASIC of an impersonation scam.

National Anti-Scam Centre – The National Anti-Scam Centre publishes news on scams, quarterly scams updates, statistics and various other publications.

ACCC's ScamWatch – The ScamWatch website provides information about common scams, how to recognise and avoid them, how to report a scam, and where to get help if you've been scammed. It also features scam alerts and consumer education resources.

ACCC's ScamWatch – Report a scam – This page allows individuals to report scams to ScamWatch.

OAIC – Identity Fraud – This page provides resources about identity fraud.

AUSTRAC - Indicators of suspicious activity for the superannuation sector – AUSTRAC have created suspicious activity indicators to help you identify potential money laundering, terrorism financing and other serious criminal activities.



ASFA Financial Crimes Protection Initiative
Fraud And Scams Toolkit