Prepared for the Department of the Treasury
30 October 2024

Implementation of the Scams Prevention Framework

Privacy Impact Assessment

Matter number 24007052

Department of the Treasury – Scams Prevention Framework – Privacy Impact Assessment

Executive Summary

1. The Department of the Treasury (**Treasury**) has commissioned the Australian Government Solicitor (**AGS**) to complete a Privacy Impact Assessment (**PIA**) to consider the potential privacy impacts of the implementation of a Scams Prevention Framework (**SPF**).

2. Background about the proposed SPF, and an outline of the scope of this PIA, are set out in Part 1 of our report.

3. This PIA is a point-in-time analysis of the exposure draft of the SPF and accompanying explanatory memorandum released on 13 September 2024.

Purpose of this PIA

4. This PIA examines how entities will handle personal information if the Parliament enacts the SPF (see Part 2). Commissioning this PIA is a key part of the activities undertaken by Treasury to identify possible privacy impacts of the implementation of the SPF, and to implement solutions to minimise or eradicate any privacy risks.

5. Additionally, this PIA facilitates compliance by Treasury with the *Australian Government Agencies Privacy Code* (**Privacy Code**), which requires Treasury to conduct a PIA for all 'high risk' projects such as implementing the SPF.

Summary of findings

6. The SPF contemplates the creation of a framework to prevent, disrupt and report on, and respond to, scams impacting Australian consumers. The definition of scam includes deception of an SPF consumer that would, if successful, cause loss or harm including obtaining personal information.

7. On balance, we think that the privacy impacts of the SPF are proportional to the public benefit of the scheme. Nonetheless, it involves substantial and mandatory collection, use and disclosure of personal information. This PIA identifies a number of additional protections that could be applied to the SPF to ensure it appropriately protects the privacy of individuals.

Purposes of the SPF

8. Treasury intends for the SPF to create a comprehensive scheme facilitating the effective collection, use and disclosure of information to combat the rapidly increasing volume and complexity of scam activity affecting Australians.

9. The SPF aims to protect Australian consumers from the harmful monetary and non-monetary impacts caused by both general and specific scam activity. Key objects of the SPF include:

   9.1. measures to prevent, detect, disrupt, respond to and report scams carried out by both Regulated Entities (**REs**) and regulators

9.2. enhancing capacity and responsiveness to manage scam activity, including by improving communication between businesses and regulators, and between businesses through regulators

9.3. improving options for consumers to respond to scams and seek redress when a victim of a scam.

10. Further information on the background of the SPF is set out in Part 1 of this PIA.

Operation of the SPF

11. The SPF will create a legislative framework for protecting Australian consumers and small businesses against scams. It implements or enables the following features:

11.1. Overarching SPF principles that apply to REs

11.2. Sector specific SPF codes applying to regulated sectors

11.3. A multi-regulator framework

11.4. Dispute resolution mechanisms.

12. The SPF contains arrangements for the sharing of information about scams by REs to regulators; between regulators within the multi-regulator model and by SPF regulators to the dispute resolution scheme. This information sharing is aimed at facilitating the overall aims of preventing, detecting, disrupting and responding to scams.

13. These information flows are discussed in detail in Part 2 of this PIA.

Summary of protections

14. Alongside the protections imposed by the *Privacy Act 1988* (Cth) (discussed in detail in this PIA, particularly in Part 3), a number of privacy protections are contained in the structure of the SPF itself.

15. These include:

15.1. The 'reasonableness' standard imported into many of the SPF's provisions applicable to REs and SPF regulators (see particularly the analysis in relation to Australian Privacy Principle (**APP**) 2 and APP 10 below)

15.2. Mechanisms included in the draft legislation to clarify what personal information it is contemplated REs will collect, use and disclose (such as the drafting notes to proposed s 58BS(2)

15.3. Restrictions on the disclosure of personal information under the legislation, such as the prescribed circumstances in which personal information may be disclosed set out under proposed s 58BU.

Summary of privacy impacts and issues

16. The collection, use and disclosure of information about scams is a core component of the SPF. As discussed in detail below, some of this information may include the personal information of victims of scams (as well as the personal information of scammers or suspected scammers).

17. Consequently, the SPF will result in increased handling of personal information, often beyond the original intentions of the individual concerned, and without their knowledge.

18. New types of personal information will be collected, primarily by REs, in order to prevent, detect and disrupt scams, as well as in fulfilment of reporting obligations to SPF regulators.

19. Data, including the personal information of potentially-vulnerable victims of scams, will also be collated in ways that may make it an attractive target for scammers.

Privacy risks and recommendations

20. Australia is a signatory to the *International Covenant on Civil and Political Rights* (the **ICCPR**) which protects against 'arbitrary or unlawful interference with privacy': Article 17.[1]

21. Importantly, not every interference with privacy will be inconsistent with the right to privacy. The concept of 'arbitrariness' is 'intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the ICCPR and should be, in any event, reasonable in the particular circumstances.'[2]

22. As the SPF will introduce new legislation which will impact on the privacy of individuals, the PIA examined whether the policy settings are reasonable, necessary and proportionate.

23. We also examined whether the SPF will enable the handling of personal information in accordance with the *Privacy Act 1988* (Cth) (the **Privacy Act**), which codifies the right to information privacy in the ICCPR into Australian law.

24. The following is a high-level summary of the findings of the PIA and our recommendations.

REs will collect, use and disclose personal information in new ways

25. The SPF imposes new obligations on REs to collect, use and disclose personal information. With these new data handling activities comes a risk of misuse, which should be mitigated by clear and effective guidance to REs (Recommendation 1).

SPF codes and delegated legislation will play an important role in the SPF

26. The SPF principles will be supported and supplemented by SPF codes for regulated sectors, which are likely to involve the handling of personal information beyond that contemplated by the exposure draft SPF, and therefore not considered under this PIA. To mitigate the risk of data misuse and other interferences with privacy, we recommend that additional PIAs be undertaken when SPF codes and important delegated instruments are implemented (Recommendation 2).

1 International Covenant on Civil and Political Rights | OHCHR

2 UN Human Rights Committee, General Comment No. 16, [4]

Some SPF provisions appear to authorise sharing of unnecessary personal information

27. We consider that provisions which appear to authorise the sharing of personal information in circumstances where it may be unnecessary to do so, contrary to the Privacy Act (such as proposed s 58BU) should be considered for amendment to clarify when personal information may and may not be shared (Recommendation 3).

The collection and use of personal information about vulnerable people under the SPF

28. The SPF will disproportionately involve the personal information of vulnerable people who may be particularly likely to fall prey to scams. Under the exposure draft SPF, the personal information of vulnerable people may be used unnecessarily to identify potential classes of people who may be more likely to fall victims of scams. There is also a potential risk of misuse of personal information to deny services to vulnerable people most likely to fall prey to scams.[3] We recommend that the draft SPF be amended to ensure that this information is not used unnecessarily, and that guidance be given to REs aimed at preventing data misuse (Recommendation 4).

Disclosure of information to overseas regulators and law enforcement agencies

29. Proposed s 58BU does not expressly authorise the SPF general regulator to disclose information to overseas regulators and law enforcement agencies. This has the effect that s 58BU(3)(b) would apply, prohibiting the SPF general regulator from disclosing personal information to these entities.

30. We recognise that scammers may reside outside Australia and that disclosing personal information to overseas regulators and law enforcement agencies may sometimes assist in achieving the purpose of the SPF. We recommend that Treasury consider inserting an additional express authorisation for this purpose into proposed s 58BU(2) rather than removing the protection in proposed s 58BU(3)(2). We further recommend that Treasury consider restricting any authorisation due to the potential loss of control of personal information disclosed overseas, and the different standards of privacy protection that may apply overseas (Recommendation 5).

Recommendations

#	Recommendation	Reference
1	Develop guidance materials to support REs to comply with privacy obligations	[185] and Annexure A
2	Complete PIA for SPF codes and delegated legislation	[189]
3	Consider if some SPF provisions should require deidentification	[192]
4	Consider altering Bill to protect vulnerable classes	[198]
5	Consider inserting into proposed s 58BU(2) an express authorisation to disclose information to overseas regulators and law enforcement agencies	[199]

[3] See the submissions of Bendigo Bank on the exposure draft SPF.

Table of contents

Part 1 – Background

31. On 5 August 2024, Treasury requested that AGS undertake a PIA to evaluate the potential privacy impacts of implementing the SPF.

32. On 30 November 2023, the Assistant Treasurer, together with the Minister for Communications, announced the SPF and released a consultation paper for the reform. The media release characterised the SPF as the next stage in addressing the 'scourge of scams', which cost Australians $3.1 billion in 2022.[4]

33. On 21 May 2024, the Assistant Treasurer, together with the Minister for Communications, further announced the allocation of $67.5 million in the 2024-25 Budget to fund the SPF. This announcement also highlighted a reduction of reported scam losses, suggesting that scam interventions implemented to date had been effective.[5]

34. On 13 September 2024, the Assistant Treasure published the Exposure Draft of the Treasury Laws Amendment Bill 2024: Scams Prevention Framework, which if enacted, would establish the SPF.

Treasury's functions

35. Treasury is a Commonwealth government department tasked with developing, delivering and implementing economic policy.[6] In particular, Treasury is responsible for developing policy on competition and consumer policy and supporting the Treasurer to administering the *Competition and Consumer Act 2010* (Cth) (**CCA**).

36. Currently, Treasury is developing the design of the SPF, which it intends to implement primarily by amending the CCA as well as sector-specific obligations through subordinate legislation.[7]

Proposed Scams Prevention Framework

37. Treasury intends for the SPF to create a comprehensive scheme facilitating the effective collection, use and disclosure of information to combat the rapidly increasing volume and complexity of scam activity affecting Australians.

38. The SPF aims to protect Australian consumers from the harmful monetary and non-monetary impacts caused by both general and specific scam activity. Key objects of the SPF include:

    38.1. measures to prevent, detect, disrupt, respond to and report scams carried out by both REs and regulators

---

4 Assistant Treasurer and Minister for Communications, Joint Media Release, *Government takes next step in fight against scams*, 30 November 2023 <Government takes next step in fight against scams | Treasury Ministers> referring to ACCC, Targeting Scams: Report of the ACCC on scams activity (April 2023) Targeting scams 2022.pdf (accc.gov.au).

5 Assistant Treasurer and Minister for Communications, Joint Media Release, *Albanese Government continues crackdown on scammers*, 21 May 2024 <Albanese Government continues crackdown on scammers | Treasury Ministers>.

6 See Administrative Arrangements Orders (as at 29 July 2024).

7 Implementing the SCF also involves amending the *Australian Communications and Media Authority Act 2005* (Cth) and *Corporations Act 2001* (Cth),

38.2. enhancing capacity and responsiveness to manage scam activity, including by improving communication between businesses and regulators, and between businesses through regulators

38.3. improving options for consumers to respond to scams and seek redress when a victim of a scam.

Individuals, entities and agencies impacted by the SPF

39. The SPF will set out obligations for private entities to prevent, detect, disrupt, respond and report to scam activity. It will feature a multi-regulator model for the administration and enforcement of the SPF. Consequently, the SPF will impact and impose responsibilities on many different parties. The table below contains a brief overview of the role of each party and their proposed responsibilities under the CCA, with mandatory obligations in **red**:

Party	Role	Key Powers/Responsibilities
Treasury Minister	The Treasury Minister will be responsible to Parliament for the effective and lawful operation of the SPF.	• Designating one or more businesses or services to be a regulated sector for the purposes of the SPF • Delegating the power to make an instrument designating businesses or services to be a regulated sector to another Minister • Designating a Commonwealth entity to be the SPF sector regulator for a regulated sector • Making SPF rules to provide further clarity on the operation of SPF provisions, such as to exclude conduct from the definition of scam • Delegating the power to designate a Commonwealth entity to be an SPF sector regulator for a regulated sector to another Minister • Making an SPF code • Delegating the power to make an SPF code to another Minister, the ACCC, or the entity that is, or is to be, the SPF sector regulator • Authorising an external dispute resolution (**EDR**) scheme for one or more sectors
Regulated Entity (**RE**)	REs must comply with overarching obligations in the SPF and relevant sector code obligations (if made) targeted at reducing harm from scams.	• Developing, implementing, and certifying governance policies and procedures in relation to addressing scam activity • Taking reasonable steps to prevent, detect, and disrupt scams activity on or related to its regulated service • Responding to scams through having appropriate dispute resolution and reporting mechanisms available to SPF consumers • Reporting information about scam activity to the SPF general and/or sector regulators
SPF general regulator	The ACCC is the SPF general regulator and will oversee the overarching SPF and	• Working with SPF sector regulators to monitor, regulate and enforce the SPF

Party	Role	Key Powers/Responsibilities
	support an ecosystem wide approach to the administration and enforcement of the SPF.	• Disclosing information to an entity to achieve the objects of the SPF • Monitoring and supervising compliance with SPF provisions through undertaking activities such as thematic reviews, investigations and enforcement of breaches • Disclosing information to SPF sector regulators and EDR scheme operators • Appointing an inspector • Reviewing and advising the Minister about the operation of SPF provisions • Obtaining information, documents ACCC's functions and powers under section 155 of the CCA (concerning the power to obtain information, documents and evidence) • The functions and powers of the SPF general regulator conferred by any other SPF provisions (for example under the Regulatory Powers Act conferred by an SPF provision).
SPF sector regulator	SPF sector regulators, currently intended to be the Australian Competition and Consumer Commission (ACCC), the Australian Securities and Investments Commission (ASIC) and the Australian Communications and Media Authority (ACMA), will regulate and enforce sector-specific obligations and any applicable sector code.	• Working with the SPF general regulator to monitor, regulate and enforce the SPF in relation to a particular sector • Disclosing information to SPF sector regulator and EDR scheme operators • Appointing an inspector
EDR scheme operator	EDR scheme operators will assist SPF consumers to seek redress if they become victim to a scam.	• Handling scam complaints from SPF consumers • Reporting to SPF regulators
SPF consumers	The SPF aims to protect SPF consumers, which includes small businesses, from scams. SPF consumers will be able to report scams and seek redress when a scam occurs.	• SPF consumers will not have responsibilities under the SPF.

Handling of personal information will increase under the SPF

40. Implementing the SPF will result in increased collection, use and disclosure of personal information in order to comply with the obligations detailed above. As

scams are usually directed towards individuals, this data will often include personal information (see Glossary). This will likely include information such as a victim's name and phone number, but may also include financial information such as bank account details. It may also include the personal information of a scammer or suspected scammer.[8]

41. Although 'financial information' does not fall within the definition of 'sensitive information' in s 6(1) of the *Privacy Act 1988* (**Privacy Act**), many Australians consider their financial information to be particularly sensitive because of the consequences if mishandled.[9] Generally, the community expects entities to give financial information a higher level of protection[10].

Actionable Scam Intelligence (ASI)

42. A key feature of the SPF is the prompt sharing of 'actionable scam intelligence' (**ASI**) to relevant parties to improve system-wide responses to scams. ASI is defined in the draft SPF as if (and when) an RE has reasonable grounds to suspect that a communication, transaction or other activity on, or relating to, a regulated service of the RE is a scam (proposed s 58AI). REs may obtain ASI from:

42.1. **Reports received directly from SPF consumer**: These reports may include personal information about the SPF consumer, such as an SPF consumer's name and contact details, or details of individuals who make a report on behalf of an SPF consumer. This may include financial information about the SPF consumer, as many scams are monetary in nature. Additionally, reports may include information about the individual carrying out the scam activity,[11] individuals associated with scammers and individuals impersonated as part of scam activity. It is expected that sector codes would set out additional detailed requirements about what must be included in a scam report, and this may differ across sectors.

42.2. **RE investigations**: Investigations may identify ASI, such as through a bank identifying unusual transactions through internal analysis. This type of ASI may comprise information about scam perpetrators and their associates, as well as aggregated data generated by analysing profiles and activity of SPF consumers. Although aggregated, this data may also contain personal information if it is not de-identified.[12] De-identified information will no longer comprise personal information where, in context, the risk of an individual being re-identified in the data is very low.[13]

---

8 We note the importance of applying adequate privacy protection to the personal information of suspected scammers – not just because the Privacy Act requires this, but also because what appears to be the personal information of a suspected scammer may in fact be the assumed identity of a victim: see IDCARE's submission on the exposure draft.

9 For example, personal information such as credit card details may be used to make unauthorised transactions.

10 See OAIC Guide to Securing Personal Information, p 13.

11 For example, in the case of an online scam, this may include details of their internet activity such as IP logins, account information, user activity, linked accounts, aliases etc.

12 For example, reports and spreadsheets generated from analysing profiles and activity for thousands of customers will still contain personal information if identifiers are not removed, despite the information being presented in an aggregated format.

13 See OAIC, De-identification and the Privacy Act, p 3.

42.3. **SPF Reports received from the SPF general regulator**: REs may receive reports from the SPF general regulator including information about ASI. These reports may pass on ASI received by the SPF general regulator from other REs made under proposed s 58BR and proposed s 58BX(2). The SPF general regulator may also pass on ASI received from non-SPF-regulated entities, such as entities overseas or Scamwatch. Reports may contain personal information about SPF consumers, individuals that make scam reports, impersonated individuals, as well as scam perpetrators and their associates.

42.4. **Other sources**: REs may also obtain ASI from other sources, including non-SPF regulators, publicly available information (e.g. news platforms) and industry bodies. For example, the Australian Taxation Office (**ATO**) may inform an RE about a scam that has come to its attention or an RE may notice a news article about a particular scam. While these channels are not covered by the SPF, information obtained through these channels may still constitute ASI for the purposes of the SPF.

Implementation of the SPF in stages

43. The SPF will set out principles-based obligations that will be implemented by amending the CCA. This will be complemented by delegated legislation and legislative instruments that designate regulated sectors, consult on and implement sector-specific codes, and prescribe EDR schemes.

44. This PIA considers the privacy impacts consequential to the enactment of the SPF in the CCA. It does not consider the privacy impacts of any activities or responsibilities resulting from amendments to any other Act, or the implementation of subordinate legislation, sector-specific codes or EDR schemes.

Why is privacy relevant?

45. Australia is a signatory to the International Covenant on Civil and Political Rights (**ICCPR**) which protects against 'arbitrary or unlawful interference with privacy'.[14] Not every interference with privacy will be inconsistent with the right to privacy. The concept of 'arbitrariness' is 'intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the ICCPR and should be, in any event, reasonable in the particular circumstances.'[15]

46. The UN Human Rights Committee has interpreted the concept of reasonableness to indicate that 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.[16] Relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted.[17] Signatories must take effective measures to ensure that:

14 International Covenant on Civil and Political Rights | OHCHR

15 UN Human Rights Committee, General Comment No. 16, [4]

16 Communication No. 488/1992, Toonan v. Australia, para. 8.3; see also communications Nos. 903/1999, para 7.3, and 1482/2006, paras. 10.1 and 10.2.

17 UN Human Rights Committee, General Comment No. 16, [8]

46.1. information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the ICCPR

46.2. individuals have the right to access and correct personal data.[18]

The role of the Privacy Act

47. The Parliament has codified the information privacy aspects of the ICCPR into Australia law via the Privacy Act.

48. The Privacy Act seeks to provide nationally consistent regulation of privacy and handling of personal information (see Glossary).[19] 'Personal information' is defined broadly to cover 'information or an opinion about an identified individual, or an individual who is reasonably identifiable … whether the information or opinion is true or not': Privacy Act, s 6.

49. The coverage of information and opinions is particularly relevant for the SPF as ASI could include the fact that an individual has fallen victim to a scam or an opinion that a person *may* have fallen victim to a scam. Both pieces of information comprise personal information. It may also include the personal information of scammers or potential scammers.

Australian Privacy Principles

50. To achieve this objective, APP entities must comply with the Australian Privacy Principles (**APPs**) in Sch 1 to the Privacy Act: see s 15.

51. The APPs detail how APP entities must handle personal information over the life cycle of the information. This includes how personal information should be collected, stored, used, disclosed, accessed, corrected and destroyed. The APPs also impose higher protections for personal information which comes within the definition of sensitive information (see Glossary).

APP entities

52. There are two types of APP entities: (1) Organisations, and (2) Agencies, which includes Commonwealth government bodies such as the ACCC, ACMA and ASIC established for a public purpose under a Commonwealth law who will make up the SPF regulators.

53. Under the SPF, most REs will be an 'organisation' for the purposes of the Privacy Act, which is defined in s 6C to mean:

(a) an individual; or
(b) a body corporate; or
(c) a partnership; or
(d) any other unincorporated association; or
(e) a trust.

[18] UN Human Rights Committee, General Comment No. 16, [10]

[19] The term personal information only applies to information about an 'individual' which is defined to mean a 'natural' (i.e. living) person. As a result, information about deceased individuals is not personal information for the purposes of the Privacy Act.

that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

54. Other REs may fall within the meaning of a small business operator (**SBO**). Generally, an SBO is an individual, body corporate, partnership, unincorporated association or trust with a turnover of less than $3 million per year: s 6D(1) of the Privacy Act. As part of the response to the recent Privacy Act Review Report, the Government has agreed-in-principle to removing the exemption in the Privacy Act covering most SBOs. If this amendment occurs, most REs will be required to handle personal information under the SPF in accordance with the Privacy Act.

Why prepare a PIA?

55. A PIA is an important tool for assessing the privacy risk of any project. It examines the lifecycle of personal information handled by a system or project to identify any potential or actual privacy issues. The PIA report will identify any potential privacy impacts an activity will have on the privacy of individuals and make recommendations on how to manage, minimise or eliminate that impact.[20]

56. However, privacy risk is more than just potential non-compliance with the privacy laws. It extends to any risk that the project will not meet community expectations, or have unmitigated, unnecessary or 'arbitrary' privacy impacts on individuals.

57. When an entity conducts a PIA at the start of a project, privacy safeguards can be in-built, and any potential privacy impacts addressed in the project's design or legal framework. This strategy can be characterised as 'privacy by design'. Privacy by design is critical to ensure that a project will be established and maintained in line with community expectations and attitudes toward privacy.

58. The 2023 Australian Community Attitudes to Privacy Survey shows that Australians are increasingly concerned about privacy risks. About 62% of those surveyed see the protection of their own personal information as a major concern.

59. Australians continue to see federal government agencies as more trustworthy than businesses when it comes to how they protect and use personal information. Within the 2023 survey, there was a reversal in the declining trust in government in this area since 2007 (67% compared to 50% in 2020). Most Australians (89%) would like government to do more to protect the privacy of their data.

Scope of this PIA

60. This PIA examines the privacy impacts arising from the proposed implementation of the SPF. It describes the activities required to comply with the SPF (Part 2) and makes recommendations to minimise potential privacy risks (Part 3).

61. For further details about the preparation and scope of this PIA, included excluded matters, see the Appendix.

62. A Glossary of terms and acronyms used in this PIA is set out at the end of this document.

[20] See definition of PIA in s 33D of the Privacy Act.

Part 2 – Information Flows

63. This part of the PIA examines how entities will collect, use, disclose, and otherwise handle personal information to comply with the SPF.

64. It examines the handling of personal information by all entities, including the SPF general regulator (ACCC), SPF sector regulators (initially the ACCC, ASIC and ACMA) and REs.

65. Most information comprising ASI will relate to potential or actual scams affecting SPF consumers, and may include personal information. While not all ASI will necessarily include personal information, this PIA proceeds on the basis that all ASI data may comprise personal information.

66. The SPF involves several facets, including designation of sectors as regulated sectors, imposition of overarching principles on REs, and information sharing between regulators. Each activity may involve handling personal information as examined in further detail below.

Activity	Description	Action
Activity 1	Designation of regulated sectors	• Collection by Treasury / disclosure by the SPF general regulator • Use by Treasury • Disclosure by Treasury / collection and use by Treasury Minister
Overarching obligations for REs and EDR scheme operators		
Activity 2	Governance obligations for REs	• Secondary use and storage by RE to develop policies and procedures • Disclosure by REs to SPF general regulator

Activity 3	Preventing scams	• Collection by REs to prevent scams
		• Use by RE to:
		  ○ prevent another entity from committing a scam
		  ○ develop resources and warnings for SPF consumers
		• Secondary use and disclosure to identify and warn higher-risk SPF consumers

Activity 4	Other RE obligations	• Collection of scams information by REs • Use of scams information and secondary use of customer information by REs • Disclosure of scams information by REs to SPF consumers • Disclosure of ASI by RE to SPF general regulator / collection of ASI by SPF general regulator • Use of scams information by SPF general regulator

Activity	Description	Action
Activity 5	Internal and external dispute resolution	• Collection, use and disclosure (between REs and SPF consumers) for internal dispute resolution • Collection, use and disclosure (between REs, EDR scheme operators and SPF consumers) for external dispute resolution • Disclosure by EDR scheme operators to SPF general regulator • Disclosure of information by SPF general regulator to EDR scheme operators to assist or enable them to perform any of its functions or powers
SPF regulators		
Activity 6	Information sharing by the SPF general regulator	• Use of scams reports by SPF general regulator • Disclosure of scam reports by SPF regulators, including to the public and relevant entities
Activity 7	Information sharing between regulators	• Disclosure between SPF general regulator and SPF sector regulators
Activity 8	Monitoring compliance with and enforcing the SPF	• Secondary use and disclosure of information collected by REs and reported to SPF sector regulator

67. In our analysis below, reforms which:

67.1. will have an impact on privacy are shaded in **orange**.

67.2. are privacy neutral or privacy enhancing are shaded in **green**.

68. Only reforms shaded in orange that will have privacy impacts are examined in Part 3.

Activity 1 – Designation of regulated sectors

69. The overarching obligations in the SPF will apply to REs. An entity will be an RE for the purposes of the SPF if it provides a regulated service, so as to fall within a regulated sector: proposed s 58AD.

70. The Treasury Minister[21] will designate a business or service to be a regulated sector: proposed s 58AC. For example, the Minister may designate that the business of banking is a regulated service, such that banking is a regulated sector. This would mean that entities that engage in the business of banking would be an RE falling within the banking sector designation.

71. Before making a designation, proposed s 58AE(1) will obligate the Minister to consider the following issues:

(a) scam activity in the sector

(b) the effectiveness of existing industry initiatives to address scams

[21] Or another Minister acting as a delegate under proposed s 58AF of the SCF.

(c) the interests of persons [who] would be SPF consumers for the sector if the instrument were made

(d) the likely consequences (including benefits and risks) resulting from making the instrument, and

(e) any other matters the Minister considers relevant.

Collection by Treasury / Disclosure by SPF general regulator

72. While we consider it unlikely, it is possible that under the SPF, Treasury and/or another agency assisting a delegate of the Minister[22] may collect and use personal information to brief the Minister about a proposed designation. Additionally, the SPF general regulator may use and disclose personal information to inform Treasury on current scams information.

Use by Treasury

73. Assuming historical scams information comprises personal information, using this data to analyse the merits of designating a regulated sector would constitute a use of personal information. For example, Treasury may analyse aggregated data to assess the effectiveness of industry resolution outcomes for victims of scams: proposed s 58AE(1)(b).

Disclosure by Treasury and DITRDCA / Collection and use by Minister

74. As the Minister is a separate APP entity under the Privacy Act, providing a brief to the Minister may involve a disclosure of any personal information within the brief by Treasury. Receiving and assessing the brief consistent with proposed s 58AE may involve the collection and use of personal information by the Minister.

75. Where Treasury collects personal information for inclusion in their own records, this will constitute a separate collection by those bodies, notwithstanding that the information had previously been collected by the SCF general regulator.

Impact

76. Activity 1 is likely to have a low privacy impact for the following reasons:

Proposal	Description	Privacy impacts
Designation of regulated sector	Minister will make a legislative instrument to designate a regulated sector	Privacy enhancing. This activity will strengthen obligations on REs in the designated sector to respond to scams. It is unlikely the instrument will contain personal information.
Disclosure from SPF general regulator to Treasury	The SPF general regulator may share information with Treasury or other agencies developing policy in relation to scams	The SPF general regulator may share historical scams data comprising personal information. This may increase handling of SPF consumer reports by entities beyond their original

[22] For example, if the Minister for Communications is delegated the power to make a determination under proposed s 58AC by the Treasurer (proposed s 58AF), Department of Infrastructure, Transport, Regional Development, Communications and the Arts (**DITRDCA**) may handle personal information under the SPF.

Proposal	Description	Privacy impacts
		scope, potentially without the knowledge of the consumer.
Use and disclosure of historical scams data	Use and disclosure of historical scams data by Treasury to prepare Ministerial brief	Privacy neutral. Generally, this activity will involve the use and disclosure of aggregated or de-identified data only. To the extent the agencies use some limited personal information to prepare a brief, this will occur within small teams with access to the data for the briefing purpose only.

Activity 2 – Governance obligations for REs

77. The governance principle will require REs to meet governance requirements detailed at proposed ss 58BC to 58BH. These obligations are designed to ensure REs have adequate policies and procedures in place to effectively manage risks caused by scams and comply with the SPF. Governance obligations include:

Section	Description
Proposed 58BC	• Documenting and implementing policies and procedures to prevent, detect, disrupt, respond and report scams addressing or having regard to the matters in proposed s 58BD. • Developing performance metrics and targets to review the effectiveness of these policies and procedures.
Proposed 58BE	• A senior officer at the RE must annually certify the policies, procedures, metrics and targets within 7 days after the start of each financial year.
Proposed 58BF	• Ensuring the RE publishes publicly accessible information about the steps the RE is taking to protect SPF consumers from scams and the rights of SPF consumers in relation to scams.
Proposed 58BG	• Keeping records for 6 years about compliance with ss 58BC and 58BE. • Keeping records for 6 years of each risk assessment outlining evidence the RE has obtained about scam-related risks.
Proposed 58BH	• Reporting policies, procedures, metrics and targets, as well as records under s 58BG, to an SPF regulator if requested.

78. These obligations may cause an RE to collect, use and disclose the following kinds of personal information.

Personal information about RE staff

79. REs may collect, use or disclose personal information about the activities of their staff and senior officers, e.g. within documents evidencing the engagement of staff and senior officers in SPF compliance activities.

Secondary use by REs

80. REs may use information obtained to comply with other aspects of the SPF to assist the RE to develop effective governance policies. For example, if a telecommunications provider identifies a new type of SMS scam through system

analysis, it may use information provided in customer reports about the scam to develop policies and procedures to respond to this type of scam.

81. Using personal information collected when responding to a specific scam to develop governance documents to respond to scams generally will involve a use of personal information for a secondary or different purpose. This is the case whether an RE obtained the information through a customer report or system analysis, or from regulators or other REs. For example, reviewing a consumer report about a scam to identify systematic deficiencies will involve using the consumer's personal information, including their opinions about the scam event. We discuss this secondary use further below under the APP 6 analysis.

Disclosure to SPF regulators

82. Proposed ss 58BG and 58BH of the SPF may result in REs disclosing personal information to SPF regulators. This risk is most likely to eventuate where an SPF regulator requests a copy of the risks assessments completed by REs to assess scam-related risks, as these risk assessments could contain personal information (e.g. if the risk assessment occurs in response to an SPF consumer report, and personal information about the SPF consumer is replicated within the assessment).

Impact

83. Activity 2 is likely to have a moderate privacy impact for the following reasons:

Proposal	Description	Privacy impacts
Secondary use of scam information	REs may use SPF consumer reports and analysis to inform governance policies	Using information to develop governance documents will occur for a secondary purpose. While such activities will support REs to better protect consumers from scan activities, it may increase handling of consumer reports by entities beyond their original scope, potentially without the knowledge of a SPF consumer.
Disclosure to SPF regulators	SPF regulators may request copies of records demonstrating compliance with governance obligations	Privacy neutral. Disclosure of records to the SPF regulator may result in disclosure of limited personal information about SPF consumers and RE staff. However, this will facilitate effective oversight by SPF regulators, which will improve actions by RE to respond to scams, which in turn, will protect personal information.

Activity 3 – Preventing scams

84. The prevention principle requires an RE to take reasonable steps to prevent another person from committing a scam relating to a regulated service of the RE: SPF proposed s 58BJ.

85. Additionally, an RE must make relevant resources accessible to SPF consumers of their service to (1) facilitate identification of scams relating to the service, and (2) minimise the risk of SPF consumers becoming a scam victim to facilitate prevention: proposed s 58BK(1). REs must also identify particular classes of SPF consumers that are at *higher risk* of being targeted by a scam: proposed s 58BK(2)(a). The

provision does not detail how REs should assess a class's risk level or what constitutes a 'higher risk'. However, REs must provide warnings about scams to SPF consumers who belong to a higher risk SPF class: proposed s 58K(2)(b).

86. Proposed s 58BL contemplates an SPF sector regulator providing guidance on the above obligations in an SPF code. This PIA does not consider any privacy impacts arising out of obligations or activities occurring pursuant to an SPF code.

Collection by REs to prevent scams

87. Proposed s 58BJ of the SPF does not specify how an RE should effectively prevent scams. The SPF contemplates that REs may be informed about scam activity through RE investigations, reports from consumers[23] or receiving ASI from another entity.

88. Information collected from consumers or other REs is likely to contain personal information. This may include consumer contact details for an individual report, or names, contact details and demographical information for ASI.

89. Additionally, REs must take reasonable steps to comply with proposed ss 58BJ(1) and 58BK(2). This requires an RE to do more than merely acting on ASI. REs will be expected to actively collect data to monitor scam trends to comply with proposed s 58BL(1). This may also involve collection of personal information, particularly if an RE is actively collecting data from SPF consumers beyond that collected through RE investigations and reports from consumers.

90. We do not consider proposed s 58BK(2) to require identification of specific SPF consumers as high risk – rather, certain *classes* are assessed as high risk (proposed s 58BK(2)(a)), and members of that class are then required to be notified (proposed s 58BK(2)(b)), irrespective of the extent to which they are in fact at risk of becoming scam victims.[24] Where it is not possible to deidentify information used to perform the proposed s 58BK(2)(a) analysis (i.e. such that the risk of re-identification is very low), use of consumer personal information may occur.

91. Additionally, the RE will collect personal information in relation to these individuals where a record is kept recording their receipt of notifications as to their risk level.

Use of information to prevent scams

92. Merely acting on scam intelligence to respond to a scam is insufficient for an RE to comply with its prevention obligations. An RE must use information it collects to inform an appropriate preventative response. Where scam intelligence contains personal information (e.g. about an individual carrying out scam activity), relying on the scam intelligence to prevent that individual holding themselves out as the RE or impersonating the RE would constitute a use of this personal information.

---

23 REs may also receive reports from non-SCF consumers as scams may be directed towards consumers who are not customers of the RE.

24 For example, older individuals generally might be identified as particularly high-risk in relation to telecommunication scams, but a particular older person might be at very low risk of falling victim to scams, for example through a high level of awareness of the risk of scams, or because they do not make use of common scam vectors, such as online banking.

Secondary use of information by REs to identify higher risk SPF consumers

93. We anticipate that REs will use existing customer records to identify higher risk SPF consumers to comply with proposed s 58BK. This may include reviewing customer records to identify risk factors, e.g. if an SPF consumer is a former scam victim, age, location, language, use of similar services, similar transactions.

94. Using existing customer information for this purpose would be a secondary use, as the RE would have collected the relevant personal information for other purposes. The permissibility of this secondary use under the Privacy Act is discussed further below.

Disclosure of scams information to higher risk SPF consumers

95. An RE is unlikely to disclose personal information to a higher risk SPF consumer to meet its prevention obligations. Section 58BK(2)(b) of the SPF requires the RE to provide warnings to these consumers. REs should not need to disclose any personal information used to identify scams to SPF consumers when providing these warnings.

Impact

96. Activity 3 is likely to have a moderate to high privacy impact for the following reasons:

Proposal	Description	Privacy impacts
Collection of information to prevent scams	REs may collect information or run analyses to prevent scams	REs may collect personal information through active data collection to comply with s 58BL(1). It is unclear what sources REs may actively collect data from, or what kinds of information could be collected, although this data is likely to be collected without SPF consumers' knowledge, carrying a high privacy risk. The privacy impact of collecting data through RE investigations, reports from consumers and from other REs is considered under Activity 4.
Use of information to prevent scams	REs may use scam information to prevent scams	Privacy neutral. REs may use RE investigations, consumer reports or analyses results to take action to prevent other entities impersonating or misrepresenting to be the RE. While this may involve the use of personal information about a consumer or a scam perpetrator, this will better protect consumers from scams and interferences to their privacy.
Secondary use of information to identify higher risk SPF consumers	REs may need to use personal information to identify higher risk SPF consumers to enable it to provide warnings	Using personal information collected for another purpose to identify higher risk SPF consumers may have significant privacy impacts due to (1) the risk of REs using this analysis

Proposal	Description	Privacy impacts
		adversely against higher risk SPF consumers, and (2) because of its attractiveness as a data source for malicious intruders.
Disclosure of scams information to higher risk SPF consumers	REs will provide warnings to higher risk SPF consumers	Privacy enhancing. REs should not need to disclose any personal information (beyond contact details) to warn higher risk SPF consumers of scam activity. These warnings will assist higher risk SPF consumers to protect themselves against scams and interferences with their privacy.

Activity 4 – Other RE obligations

97. To comply with their detection obligations (SPF principle 3), an RE must take reasonable steps to detect scams, both during and after a scam occurs: proposed s 58BN. Additionally, an RE must, within a reasonable time, identify the SPF consumers impacted by the scam and the nature of the impact: proposed s 58BO.

98. To comply with their reporting obligations (SPF principle 4), an RE must report ASI or scam reports to the SPF general regulator: proposed ss 58BR(1) and 58BR(2). An RE must report ASI within a set time period (determined in the SPF rules) from when the intelligence becomes actionable scam intelligence for the entity and give a scam report upon request from an SPF regulator: proposed s 58BS(1). The SPF general regulator may approve by way of notifiable instrument the report form and contents: proposed s 58BS(2).

99. To comply with their disruption obligations (SPF principle 5), an RE must take reasonable steps to disrupt actual or suspected scams relating to ASI held by the RE, or to prevent loss or harm (including further loss or harm) arising from the scam: proposed s 58BW.

100. Disrupting a scam requires an RE to take reasonable steps within a reasonable time to disclose information to SPF consumers to alert them to a suspected or actual scam, as informed by ASI: proposed s 58BX(1).

101. REs may enjoy safe harbour protection when acting to disrupt a suspected scam while it is investigating the nature of the suspected scam activity. This protection applies for a period starting the day intelligence becomes ASI and ending when the entity identifies whether the activity is a scam, or after 28 days, whichever is the earlier: proposed s 58BZ.

102. RE's must share information as a scam investigation report with the SPF general regulator at the end of the safe harbour period: proposed s 58BX(2)-(5). This report should cover the findings from the RE's investigation into the suspected scam activity. If the RE reasonably believes it is a scam, the RE must set out the loss or harm that has resulted from the scam, any disruptive action the RE took and whether those actions have been reversed. If, after investigation, the RE reasonably believes the activity was not a scam, the report must specify the disruptive actions taken and whether those actions have been reversed.

103. RE obligations to respond to scams (SPF principle 6) include that an RE must have an accessible mechanism for their SPF consumers to report scams to the RE: proposed s 58BZB.

Declarations about scam activities that are eligible data breaches

104. Additionally, the proposed enactment of the eligible data breach declaration provisions in the Privacy and Other Legislation Amendment Bill 2024 (Cth) may impact on how REs and SPF regulators can handle personal information. For example, if a declaration is made about scam activity that constitutes an eligible data breach, an APP entity will not have to comply with the APPs or any obligation of confidence when undertaking specified activities authorised by the declaration, such as collecting certain kinds of personal information to reduce harm to victims of the scam.

105. This PIA does not consider how these proposed provisions may impact on RE and SPF regulator handling of personal information, or how the eligible data breach declaration provisions operate alongside the SPF.

Collection of scams information by REs

106. REs may collect personal information to detect and respond to scams. REs will receive reports from consumers notifying the RE of current scams. The RE reporting mechanism is likely to collect personal information such as a consumer's name, contact details and account number, and also include information about scam perpetrators and the mechanisms used to perpetrate the scam (e.g. SMS, email).

Use of scams information and secondary use of customer data by REs

107. REs will need to act on scam reports and ASI to effectively detect and disrupt scams. For example, a bank may delay sending push authorisations for transaction requests if it has received several scam reports about a particular bank account. Taking action to detect and disrupt scam activity will require use, and potentially disclosure, of customer data collected for a service delivery purpose.

108. Using existing customer data to detect and disrupt scams may result in a significant interference with privacy, both through additional handling of personal information, and where the RE withholds services while a scam investigation occurs (e.g. by a bank pausing transactions to an account it suspects is associated with scam activity).

109. REs must act reasonably and in good faith to benefit from the safe harbour provision. At a minimum, an RE must conduct an investigation and analysis of scam reports and ASI received from other entities to satisfy itself that information about a suspected scam is genuine. This may require the RE to review the activity of any, or all of its SPF consumers, personal information which consumers may expect the RE to use to provide services only.

110. Similarly, compliance with RE obligations under proposed s 58BO, to identify impacted SPF consumers within a reasonable time will necessitate use of existing customer transaction records and activity. Related to the previous activity, REs must give resources and warnings to SPF consumers to prevent scams: proposed s 58BK.

Disclosure of scams information by REs to SPF consumers

111. REs must disclose information about a suspected scam to SPF consumers to comply with proposed s 58BX(1) of the SPF. While REs will use existing information and contact details to send a scams notification to an SPF consumer, REs are unlikely to disclose personal information within a scam notification. Rather, an RE is more likely to distil the substance of scam information and provide general guidance information to enable SPF consumers to protect themselves.

Disclosure of ASI to SPF general regulator / collection of ASI by SPF general regulator

Proposed s 58BR

112. REs will disclose personal information when reporting to the SPF general regulator under proposed s 58BR either at the start of the safe harbour period or in response to a written request from the. This will also constitute a collection of information by the SPF general regulator.

113. The SPF general regulator anticipates requesting scam reports under proposed s 58BR(2) in circumstances including:

113.1. to respond to wide spread or multi-victim scams

113.2. where there are high-loss victims

113.3. to better understand novel or emerging scam activity, and

113.4. to support compliance monitoring and enforcement activity.

114. SPF sector regulators may also request a scam report from REs operating in the sector regulated by the SPF sector regulator.

115. The SPF general regulator may prescribe the form, and kinds of information for inclusion in a proposed s 58R report: proposed 58BS. While the specific kinds of information for inclusion will be specified in future SPF codes or legislative instruments, reports will likely contain SPF consumer personal information, including names, contact details, bank account details and/or credit card details, as well as information about scam perpetrators.

Proposed s 58BX(2)

116. REs will also disclose personal information when reporting to the SPF general regulator at the end of the safe harbour period under proposed s 58BX(2). This will also constitute a collection of information by the SPF general regulator.

117. Proposed s 58BX(3) of the SPF contemplates collection of personal information (such as names, contact details, bank account details and credit card details) of:

117.1. persons who commit scams (or are associated with those individuals)

117.2. a person impersonated as part of a scam

117.3. SPF consumers who are victims of scams, and

117.4. individuals who report scams on behalf of SPF consumers (e.g. family members).

Use of scams information by SPF general regulator

Proposed s 58BU

118. Use and disclosure of scams information under proposed s 58BU are discussed under Activity 6.

Section 58BX

119. The SPF general regulator may use scam investigation reports received from REs under proposed s 58BX at the end of the safe harbour period. This may include using reports to analyse scam activity at an economy-wide or systemic level. As reports from REs will likely contain personal information, this would constitute a use personal information.

Impact

120. Activity 4 is likely have a moderate to high privacy impact for the reasons below:

Proposal	Description	Privacy impacts
Collection and use of reports to detect and disrupt scams	REs will collect and use reports from consumers to detect and disrupt scams	REs may collect new kinds of personal information with consumer scam reports. While REs will usually collect and use consumer reports with the implied consent of the consumer, they will contain detailed information about vulnerable consumers.
Secondary use of customer data to detect and disrupt scams	REs may run analyses on existing customer data to detect and disrupt scams, including to identify SPF consumers who have been impacted by scams.	Secondary use of customer data to detect scams and identify victims of scams significantly interferes with privacy. REs may need to review consumer activity without the knowledge of SPF consumers, who would expect REs to use this information to deliver services only.
Disclosure of scams information to SPF consumers	REs will provide SPF consumers with information to assist them to act in relation to suspected scams.	Privacy enhancing. REs should not need to disclose any personal information (except contact details) to comply with proposed s 58BX(1). This proposal enhances privacy by enabling SPF consumers to reduce the risk of unwanted interference by scammers.
Disclosure of scams information to SPF general regulator	The RE will disclose personal information when reporting ASI or making scam reports at the start of the safe harbour period. This also constitutes a collection by the SPF general regulator.	This proposal will result in increased handling of personal information. SPF consumers may not be aware of these activities, particularly where a report relates to ASI. These reports will gather information about vulnerable SPF consumers.

Proposal	Description	Privacy impacts
Disclosure of scam investigation reports to SPF general regulator	REs must disclose information on ASI and related their disruption actions to the SPF general regulator in an approved form at the end of the safe harbour period.	RE reports to the SPF general regulator under proposed s 58BX(2)-(5) will likely contain personal information. This may result in the SPF regulator collecting significant volumes of personal information about affected and vulnerable SPF consumers.
Use of scams information by SPF general regulator	SPF general regulator may use information to analyse scams at systemic or cross-sectoral level.	Information is limited as to how the SPF general regulator might engage in its own disruptive activities, however, this may constitute a notable risk to privacy if personal information is being analysed to identify scam risks.

Activity 5 – Internal and external dispute resolution

Internal dispute resolution

121. The respond principle requires REs to have an accessible and transparent internal dispute resolution mechanism to enable SPF consumers to complain about scams: proposed s 58BZC. The internal dispute resolution process would involve collection and use of personal information to resolve the dispute. The SPF codes may set out additional conditions related to internal dispute resolution: proposed 58BZE(b).

EDR schemes

122. The respond principle also requires RE to be a member of an EDR scheme that is authorised by the Minister for their regulated sector: proposed s 58BZD(1).

123. The Minister may, by legislative instrument, authorise an EDR scheme for each regulated sector to assist SCF consumers to seek redress if they become a victim to a scam: proposed s 58DB. The SPF codes may set out additional conditions related to EDR: proposed s 58BZE(c).

124. An EDR scheme operator will collect, use and disclose personal information to resolve a complaint from an SPF consumer. This includes personal information the EDR scheme operator will share with, or obtain from the RE so that the RE can effectively participate in the EDR process. Similarly, an RE will handle SPF consumer personal information to effectively participate in the EDR process.

125. The SPF general regulator or the SPF sector regulator may also disclose information to the EDR scheme operator for the purposes of enabling or assisting the EDR operator to perform any of its functions or powers: proposed s 58DE. This may involve disclosing personal information.

126. The SPF EDR scheme operator will be required to report certain information to SPF regulators under proposed s 58DD(1) if they become aware:

126.1. that there have been serious contraventions of any law in connection to a complaint

126.2. that a party to the compliant has failed to give effect to the EDR scheme operator's determination, and

126.3. of any systemic issues arising from the consideration of complaints.

127. The SPF EDR scheme operator must give particulars of these matters to the SPF regulators and this will involve disclosing personal information.

128. The SPF EDR scheme operator may also give particulars of a settlement of a complaint to the SPF general regulator and relevant SPF sector regulator if the SPF EDR scheme regulator thinks the settlement may require investigation: proposed s 58DD(2).

Impact

129. Activity 5 is likely to have a low to moderate privacy impact for the reasons below:

Proposal	Description	Privacy impacts
Collection, use and disclosure for internal dispute resolution	REs will collect, use and disclose personal information to respond to complaints and requests for internal review	Privacy enhancing. The internal review proposal will result in REs handling limited additional personal information with the SPF consumers consent. Importantly, this proposal empowers consumers to seek redress for interferences to their privacy.
Collection, use and disclosure by EDR scheme operators, and by REs as part of EDR process	EDR scheme operators and REs will collect, use and disclose personal information to provide, or participate in, an EDR service.	Privacy neutral. While this proposal increases handling of personal information, this will largely occur with the consent and knowledge of an SPF consumer. The proposal also assists SPF consumers to seek redress for interferences to their privacy.
Disclosure by SPF regulators to EDR scheme operators	SPF regulators may disclose personal information to EDR scheme operators to enable or assist them to perform any of its functions or powers	Privacy neutral. SPF regulators may disclose some personal information to EDR scheme operators where disclosing the information reasonably enables or assists the SPF EDR scheme operator to perform its functions or powers. This proposal will improve the ability of SPF consumers to seek redress, including in relation to interferences to their privacy.
Disclosure by EDR scheme to SPF regulators	EDR scheme operators will report personal information to SPF regulators enable enforcement activities or identify systemic issues.	While intended to ensure the EDR scheme operators can carry out their functions effectively, this proposal carries some privacy risk if EDR scheme participants are not appropriately informed about how their personal information will be disclosed or used for secondary purposes.

Activity 6 – Information sharing by the SPF general regulator

130. A key feature of the SPF is mandatory reporting and disclosure obligations to support the flow of information relating to scam activity across the ecosystem and promote a coordinated response to scams.

131. The first aspect of the report principle will require REs to report ASI or scam reports to the SPF general regulator: proposed s 58BR. This is considered under Activity 4.

132. The second aspect of the report principle will enable the SPF general regulator to disclose information about a 'scamming action' to another person if the SPF general regulator reasonably believes that doing so will assist in achieving the objects of the SPF: proposed s 58BU.

133. A 'scamming action' includes a scam as defined in the SPF or a scam as within the ordinary meaning of the word. Sub-section 58BU(2) confirms that this obligation may capture disclosure to other regulators, Commonwealth agencies, States and Territories agencies and other persons (which may include a legal person), but this list is non-exhaustive. Sub-section 58BU(3) prohibits the SPF general regulator from disclosing information if the SPF general regulator reasonably believes:

133.1. the disclosure risks prejudicing or compromising an ongoing investigation by a law enforcement agency; or

133.2. the disclosure is to another person that is not an RE and is of personal information.

Use of scam reports by SPF general regulator

134. The SPF general regulator will use reports from REs to support its efforts to disrupt scams, as well as for the purposes of activities 7 and 8. Disruptive activities may include analysing reports to identify trends and other impacted entities. While this use may not focus on the personal information of SPF consumers, it still constitutes a use of personal information.

135. The SPF general regulator may use information to publish reports or notices about scamming actions to assist the public to disrupt and protect themselves against scamming actions.

136. To the extent the SPF general regulator uses reports for a compliance or enforcement purposes, this will involve a secondary use of personal information. Compliance and enforcement activity fall outside the scope of this PIA.

Disclosure of scam reports by SPF general regulator

137. The SPF general regulator may disclose personal information under proposed s 58BU. This could be a very broad power due to the broad definition of a 'scamming action'. Sub-section 58BU(3) expressly contemplates that personal information will be disclosed to other regulators, Commonwealth agencies, REs, law enforcement agencies, States and Territories and REs.

138. In particular, the SPF regulator will have a crucial role in facilitating information sharing between businesses through regulators. Enabling sharing of information across the ecosystem is a key objective of the SPF.

139. Disclosure of personal information will not be permitted to businesses that are not REs.

Impact

140. Activity 6 is likely to have a high privacy impact for the following reasons:

Proposal	Description	Privacy impacts
Disclosure by RE and collection by SPF general regulator	The RE will disclose personal information when reporting ASI or making scam reports at the start of the safe harbour period. This also constitutes a collection by the SPF general regulator.	This proposal is considered under Activity 4.
Use and secondary use by SPF general regulator	The SPF general regulator will use reports to disrupt scam activity. It may also use these reports for compliance and enforcement.	Similar to above, SPF consumers may be unaware of the handling of their personal information for these purposes. While this proposal improves systemic privacy, it significantly impacts on the privacy of individual SPF consumers.
Disclosure by SPF general regulator	The SPF general regulator may disclose information about a scamming action if this would achieve the SPF objects.	This proposal carries significant privacy risk. The provision expressly contemplates disclosure of personal information to many parties for a variety of purposes.

Activity 7 – Information sharing between regulators

141. Central to the SPF's multi-regulator model is a comprehensive information sharing arrangement between the SPF general regulator and the SPF sector regulators. The SPF general regulator must enter into an arrangement with each SPF sector regulator relating to the regulation and enforcement of the SPF, whether via a single arrangement with all SPF sector regulators or by having individual arrangements with each sector regulator: proposed s 58EE. A regulator that is party to such arrangements must publish them on their respective websites: proposed s 58EE(4).

142. Proposed s 58EF provides a broad power to both the SPF general regulator and SPF sector regulators to disclose information to each other. The provision authorises disclosure of 'particular information or documents', or 'information or documents of a particular kind', that are in the regulator's possession and relevant to the operation (including the enforcement) of the SPF. While the power in s 58EF is expressed in broad terms, the draft Explanatory Memorandum for the Bill suggests regulators will make disclosures under proposed s 58EF:

142.1. for the purposes of notifying another SPF regulator of action being taken to avoid dual action, or

142.2. where the recipient SPF regulator could use or act upon the information in some way to support their role in administering and enforcing the SPF.

143. Importantly, a regulator may make a disclosure on request or on its own initiative: proposed s 58EF(2).

143.1. The power to disclose to another SPF regulator is not mandatory. The SPF regulator must have regard to the object of the SPF when deciding whether to make a disclosure: proposed s 58EG.

143.2. An SPF regulator does not need to notify any person to exercise its information sharing power: proposed s 58EH.

144. Section 58EI of the SPF details the types of information that need not be disclosed, such as documents surrounding a regulator's internal administrative functions. Personal information is not listed in this provision. This suggests, consistent with the note at proposed s 58EF(2), that SPF regulators may disclose personal information when exercising their information sharing powers.

145. Any disclosure made by an SPF regulator to another SPF regulator containing personal information would also constitute a collection of personal information by the receiving SPF regulator.

146. Activity 7 only considers the disclosure aspect of the information sharing powers. While the receiving SPF regulator will likely use the information shared, we consider potential privacy impacts under other Activities such as Activity 4.

Impact

147. Activity 7 is likely to have a high privacy impact for the following reasons:

Proposal	Description	Privacy impacts
SPF regulators entering into arrangements	SPF regulators must enter into arrangements relating to the oversight of the SPF.	This proposal may impact on privacy as the arrangements may include obligations between regulators to disclose personal information. This is, however, subject to the SPF rules and not examined in this PIA.
Disclosure by SPF regulators to other SPF regulators	SPF regulators may disclose information to other SPF regulators if it is relevant to the operation or enforcement of the SPF.	This proposal carries a high privacy impact. The SPF contemplates that SPF regulators may share personal information under proposed s 58EF. This disclosure power is very broad and SPF regulators do not need to notify SPF consumers of the disclosure of information.

Activity 8 – Monitoring compliance with and enforcing the SPF

148. The SPF contains significant monitoring and compliance powers. Both the SPF general regulator and SPF sector regulators are authorised to appoint an inspector for to ensure REs comply with the SPF: proposed s 58FB.

149. Sections 58FD to 58FF of the SPF relate to monitoring or investigating compliance with an SPF code. These provisions operate by drawing on the powers in the *Regulatory Powers (Standard Provisions) Act 2014* (Cth). This PIA does not consider the privacy impacts of these provisions.

150. The SPF further details that possible penalties for non-compliance by REs include infringement notices, enforceable undertakings and injunctions. These may apply where an RE breaches an overarching obligation that is a civil penalty provision. An SPF regulator may use personal information collected for the purposes of other activities (e.g. disrupting scam activity) for compliance and enforcement purposes. The SPF general regulator may also issue public warning notices of suspected contraventions (principles or codes), give remedial directions to entities to comply with a principle or code if it reasonably suspects a failure to comply, and or make an adverse publicity order against a person who has been ordered to pay a pecuniary penalty (s58FZA to 58FZC).

Impact

151. As the compliance and investigation powers for SPF sector regulators regarding an SPF code are out of scope, and any compliance or investigation powers for the SPF general regulator are under review, the privacy impacts of these activities are not examined in detail in this PIA.

Part 3 – Privacy analysis

152. This part of the PIA examines privacy issues raised by implementing the SPF. It examines:

152.1. the potential privacy impacts and any harm that might be caused; and

152.2. recommendations to eradicate, mitigate or minimise these impacts

Privacy – a balancing exercise

153. Consistent with Australia's obligations under the ICCPR, we have considered in Part 3 whether an interference with the privacy of an individual will be reasonable, necessary and proportionate: see Background discussion.

154. We have also examined whether the proposed SPF will enable the handling of personal information in accordance with the Privacy Act, which codifies the right to information privacy in the ICCPR into Australian law.

155. Intrinsic to the Privacy Act is the balance that is sought to be achieved between the interests of the individuals and those of the entities the legislation regulates. This is reflected in the objects of the Privacy Act which recognise that the protection of the privacy of individuals is to be balanced with the interests of entities to be able to carry out their functions or activities: see s 2A(b).

Purpose of the SPF

156. Australians lost $2.7 billion to scams in 2023, with $1.3 billion of these losses resulting from investment scams. In addition to reported losses, the National Anti-Scam Centre (**NASC**) estimates that about 30% of scam victims do not report scams to anyone.[25]

157. By implementing the SPF, the Australian Government aims to better protect Australians from scam activity and losses, and to improve redress options for Australians who become a victim of a scam. The SPF is designed to achieve these objectives by improving Australia's capability to detect, disrupt, report and respond to scams, both at a systemic and individual level. The SPF imposes overarching obligations on REs to ensure REs take reasonable steps to protect and assist their customers. The SPF also authorises SPF regulators to share information, and to monitor compliance with and enforce the SPF to ensure it operates effectively.

158. Section 58AA of the SPF details that 'the object of [the SPF] is to establish a framework to protect against scams'. This confirms that the SPF is intended primarily to operate to protect Australians. We have also considered other documents associated with drafting the SPF provisions, such as the draft explanatory memorandum, in considering the purpose of specific SPF provisions.

[25] ACCC, Targeting Scams: Report of the National Anti-Scam Centre on scams activity (April 2024) Targeting scams: report of the ACCC on scams activity 2023. .

Privacy impacts and protections

159. The SPF will significantly impact on the privacy of individuals. Due to the wide-scale nature of these impacts, it is necessary to identify and weigh potential impacts against privacy benefits and protections.

160. Nonetheless, the SPF, by design, seeks to protect against scam activity that targets misuse of personal information. The definition of 'scam' in proposed s 58AG reflects that loss or harm may comprise activity which obtains personal information through deception. Depending on the sensitivity of the information, a scammer obtaining information alone may be enough to cause loss or harm e.g. if published.[26]

161. An overview of these matters, as well as the overall privacy benefits of the SPF, are set out in the tables below.

Potential privacy impacts

Impact	Description
Vulnerable individuals	• The SPF is likely to disproportionately handle personal information of vulnerable individuals who are more susceptible to scams (e.g. not native English language speakers, people with low levels of literacy of education, seniors, people with impaired intellectual functioning). • For example, this may lead to increased collection and retention of personal information about users more susceptible to scams, increasing the exposure of these cohorts to privacy harms (i.e. in the event of a data breach).[27]
Loss of choice or control	• The SPF authorises collection, use and disclosure of personal information without the consent of individuals, including for suspected scammers and victims of scams. • Consumers may not be aware or receive notice of the handling of their personal information for an SPF purpose (e.g. to prevent, disrupt or respond to a scam) • Some provisions within the SPF expressly authorise the collection of personal information by SPF regulators without notifying affected individuals.
Function creep	• REs may use and disclose existing customer records, collected to deliver services to a consumer, or to 'profile' customers at risk of scam activity, for a new 'secondary' purpose unanticipated at the time of collection (i.e. to comply with the REs SPF obligations).
Overhandling	• REs and SPF regulators may collect, use and disclose personal information additional to what they need to protect against scams. • This may unnecessarily increase privacy impacts of the SPF e.g. if unauthorised access, use or disclosure occurs.

[26] The submission from the Business Council of Australia was not supportive of the definition of scam referring to 'obtaining personal information' as a form of loss or harm due to the potential that this may conflate obligations under the SPF with requirements under the Notifiable Data Breaches (**NDB**) scheme in Pt IIIC of the Privacy Act. We observe that these obligations would be mutually exclusive, as generally the NDB obligation would apply where an APP entity has suffered a data breach, whereas the SPF reporting obligations would relate to scams against SPF consumers.

[27] See submission from the App Association.

Impact	Description
Data accumulation	• REs and the SPF regulators will collate reports collected from consumers and other analyses to obtain ASI. • REs may maintain databases of higher risk consumers. • These collections of information may present an attractive target for scammers as it collates information on consumers who are particularly vulnerable to scams, and on the success of different types of scams.
Sharing and retention by multiple entities	• ASI shared between REs and SPF regulators may result in multiple entities holding records of the same information. • Long term storage of information such as consumer reports and ASI by multiple entities increases the risk of unauthorised access or disclosure of personal information.
Misuse of personal information	• Some aspects of the SPF present a high level of risk of misuse of personal information for purposes other than those intended under the SPF. • E.g., REs who identify a consumer as higher risk as required by proposed s 58BK may misuse this information to limit product offerings to the consumer to reduce compliance risk.
Reduction in privacy protections	• Regulated entities may seek to comply with the requirement to take reasonable steps to detect scams by compromising protections which enable the handling of de-identified personal information, such as end-to-end- encryption in messages.[28]

Protections applying to these privacy impacts

Protection	Description
Standard of reasonableness throughout SPF	• The SPF imports a standard of reasonableness into most overarching obligations applying to REs. • This standard of reasonableness improves privacy protections by obligating REs to modify their handling of personal information to what is reasonable in the circumstances. • Examples of this protection in practice are available in our analysis of APPs 2 and 10.
Mechanisms available to control collection of personal information	• Some provisions in the SPF clarify what personal information is reasonable and relevant for REs to collect, use or disclose, or contemplate an SPF regulator providing this guidance in delegated legislation. • These provisions protect privacy by mitigating the risk of unnecessary over-handling of personal information.
Restrictions on disclosure of personal information	• Section 58BU protects privacy by restricting the disclosure of personal information to only some recipients. • This protects privacy by limiting the handling pf personal information.

[28] See submission from the App association.

Privacy benefits resulting from implementing the SPF

Benefit	Description
Improvements to Australia's systemic response to scams to prevent harm	• While the SPF increases handling of personal information, this will assist REs and SPF regulators to improve the effectiveness of systemically responding to scams. • Stricter governance obligations will ensure REs are better equipped to prevent, detect and disrupt scams. • Information sharing between SPF regulators, REs and other parties will improve awareness of current scam activity, allowing for a coordinated response to limit the spread of scams. • These activities will prevent or minimise harm to consumers, including harm arising from privacy interference.
Limiting the ability of scammers to misuse personal information	• Implementing the SPF will reduce the amount of personal information scammers can obtain, reducing the misuse of personal information. • Rapid response times to combat scams should also limit the harm a scammer is able to inflict on an SPF consumer if they do obtain access to personal information.
Improved redress options for SPF consumers who become scam victims	• Scam victims currently bear most of the losses from a scam with limited options for redress. For example, ASIC reported that for banks other than the 4 major banks, 96% of scam losses are born by the reviewed bank customers. Scam victims who complained to the reviewed banks were more likely to receive some form of reimbursement, with the overall share of scam loss reimbursed and/or compensated at 7% for customers who complained, compared to a share of 2% for those who did not submit a complaint.[29] • The SPF will enhance opportunities for SPF consumers to seek redress in relation to scams by having clear obligations on REs to address scams, have a transparent and accessible IDR mechanism in place and become a member of a prescribed EDR scheme. This will empower SPF consumers who become scam victims to seek redress where REs have not met their obligations and encourage REs to improve their practices to prevent scams and minimise consumer losses from scams where they do occur.

International experience

162. Scams are a global issue that impacts on consumers across all jurisdictions. The actions of other jurisdictions to respond to scams provides useful guidance on alternative options available to achieve the objectives of the SPF.

United Kingdom

163. The United Kingdom (**UK**) Government released a 'Fraud Strategy' in 2023 which aims to reduce fraud by 10%. The Fraud Strategy details how the UK Government intends to prevent, detect and disrupt scams, as well as enhancing reporting and redress systems. However, the Fraud Strategy is more the UK Government's plan for the future, rather than legislative provisions like the SPF.

[29] ASIC, 'Anti-scam practices of banks outside the four major banks' (Report 790, August 2024) Report REP 790 Anti-scam practices of banks outside the four major banks.

164. Similar to the current position in Australia, the UK has sector-specific obligations for the telecommunications, digital platforms and retail banking sectors. Commitments in these charters may be mandatory or voluntary.

165. A unique aspect of the UK response to scams is the strong redress options available to victims of authorised push payment scams. Section 72 of the *Financial Services and Markets Act 2023* (UK) requires the Payment Systems Regulator to draft and publish requirements on Payment Service Providers (**PSPs**) to reimburse customers who suffer losses due to a scam. The reimbursement requirements commenced on 7 October 2024, with a maximum reimbursement of £85,000 per claim.

166. While the UK policies significantly differ from the redress options proposed in the SPF, the business response in the UK to the policies provides an insight into how the SPF may change the behaviour of REs. In particular, where an RE faces the risk of sharing the losses from scams:

166.1. the RE may be more likely to invest in technologies and improve policies to protect their consumers and minimise losses; and

166.2. the RE may be more likely to refuse to offer high-risk services. For example, some banks in the UK have banned their customers from sending money to cryptocurrency exchanges due to the high risk of fraud.[30]

167. We have considered the potential privacy impact of RE responses to the SPF in our APP analysis below.

Singapore

168. In October 2023, the Monetary Authority of Singapore, together with the InfoComm Media Development Authority, consulted on the 'Shared Responsibility Framework'. This Framework is intended to clarify how financial institutions, telecommunications operators and consumers should share losses that result from unauthorised transactions. The Framework would apply to unauthorised transactions arising from phishing scams, with consumers bearing losses unless the financial institution or telecommunications operator has breached their anti-scam duties.

Community Expectations and Public Submissions

169. A key aspect to the balancing exercise involves consideration of community attitudes and expectations. Consistent with the objects of the Privacy Act, the Australian community expects that the benefits of any new measure will outweigh any intrusion, and that the risks of harm from the measure will be limited. Additionally, in the 2023 Australian Community Attitudes to Privacy Survey, participants overwhelmingly stated that they would like both businesses and government to do more to protect their data (p 42).

170. In November 2023, Treasury released a consultation paper entitled 'Scams – Mandatory Industry Codes'. The consultation period ran from 30 November 2023 to 29 January 2024. The submissions received during this consultation provide an insight into the community's expectations with respect to scam regulation.

[30] Australian Broadcasting Corporation, While Australian banks refuse most scam victims refunds, the UK is making them mandatory - ABC News.

171. IDCARE's submission on the consultation paper is particularly relevant as it discusses previous concerns raised by community members who have sought IDCARE's support after becoming victim to a scam. IDCARE's submission highlights the following aspects of the proposed SPF as potentially concerning to the community:

No.	Privacy concern
1.	The risk of consumers suffering additional harm after reporting a scam due to REs denying product offerings, including by REs who are informed of a consumer's association with a scam (suspected scammer or victim) through information sharing.
2.	The risk of shared scam reports being used to 'flag' an SPF consumer's account without their knowledge, leading to legitimate transactions being denied.
3.	Fears of data accumulated by REs and regulators being hacked due to poor security practices, and then misused by scammers to perpetrate further harm.
4.	A general failure to keep SPF consumers informed about how their personal information is being used to improve outcomes both for them individually and systemically.

172. IDCARE's submission also highlights the organisation's 'great success with obtaining the consent of victims and sharing details with financial institutions'. This indicates that, in principle, community members may support the SPF if assured that the operation of the SPF will not expose them to further interferences with their privacy. Other submissions, such as the ACCC submission, reiterate the need for 'trauma informed approaches' to victims to ensure victims receive necessary support and do not suffer further harm from the operation of the SPF.

173. Treasury also provided a further tranche of submissions on the exposure draft SPF. The views of these bodies and their members demonstrate community expectations surrounding privacy and the potential privacy impacts of the SPF. For their relevance to issues discussed in this PIA, we particularly highlight:

173.1. Legal Aid Queensland's submission that information collected under the SPF should be used only for its intended purpose in combatting scams;

173.2. That the identification of vulnerable customers may lead to an unintended consequence of de-banking or denial of service of higher-risk consumers, as highlighted in Bendigo Bank's submission; and

173.3. The risk that the collection of large volumes of personal information could create a 'honey pot' of data that becomes a target for theft (Customer Owned Banking Association's submission).

174. IDCARE also provided a further submission on the exposure draft which also merits comment. In its submissions, IDCARE raised concerns that the SPF is insufficiently aligned with the Privacy Act framework and the APPs. As set out above at [54], if proposed amendments to the Privacy Act take effect, all REs will be APP entities subject to the requirement in s 15 of the Privacy Act not to do an act, or engage in a practice, which breaches an APP.

175. Additionally, as our analysis below makes clear, we disagree, in that we think it is possible for REs to comply with the APPs while fulfilling their obligations under the SPF. At several points, however, this PIA does identify particular activities that might

involve REs attempting to comply with their SPF obligations in ways that breach the APPs – the Guidelines suggested under Recommendation 1, and collated at Annexure A to this advice, are designed to reduce this risk.

176. IDCARE also suggests that SPF PIAs be made public. Whether to take this course is a matter for Treasury, noting that any such publication would constitute a waiver of the Legal Professional Privilege Treasury would otherwise hold in this advice. On the other hand, publication of PIAs may engender greater community confidence in the SPF, and the actions of the Australian Government to put mechanisms in place to protect the privacy of its citizens.

Opinion

177. On balance, we think the privacy impacts of the proposed SPF will be proportionate to the public benefit resulting from protecting Australians from scam activity and facilitating a whole-of-economy response to scams.

178. The SPF will increase the handling of personal information by REs and SPF regulators. REs will need to collect, use and disclose additional personal information to comply with their overarching obligations. SPF regulators will collect, use and disclose personal information, including for compliance and enforcement purposes.

179. However, implementing the SPF will result in a strong public benefit given the significant cost of scam activity to the economy, community and affected individuals. The SPF will improve the effectiveness of government and business activities to respond to and prevent scams. The SPF will inform SPF consumers about scams to enable them to protect themselves and will establish dispute resolution pathways to assist consumers to resolve disputes with REs involving scams. The information sharing and reporting obligations under the SPF will assist REs and SPF regulators by ensuring these entities receive timely information about current scams in order to take disruption activity.

180. The SPF incorporates measures that aim to protect privacy and minimise the privacy impact of implementing the SPF, including:

180.1. importing a standard of reasonableness throughout the overarching obligations;

180.2. empowering SPF regulators to prescribe the kinds of information that REs should collect where appropriate, aiming to minimise unnecessary data collection;

180.3. for some provisions (such as s 58BU), restricting the disclosure of personal information.

181. Nonetheless, we consider that Treasury can take further steps to protect the privacy of individuals. We have summarised these below and address these in full in our detailed analysis of how the SPF interacts with individual APPs.

Guidance materials

182. Many obligations imposed on REs under the SPF require an RE to handle personal information. As REs risk civil penalties for failing to comply with their overarching obligations, there is a significant risk that REs will collect, use and disclose more

information than is necessary to comply with their obligations. Chiefly, REs may overreport information to the SPF regulators to avoid liability for non-compliance.

183. Key to minimising this risk is to ensure that REs are aware of how they should handle personal information under the SPF. This could occur by SPF regulators publishing guidance materials, either administratively or under a provision within the SPF,[31] to assist REs to comply with their obligations. These guidance materials could:

183.1. clarify what kinds of information SPF regulators expect REs to collect, use and disclose, and where this is unnecessary

183.2. provide guidance on the intersection of the responsibilities of REs under the SPF and the Privacy Act, in particular under the Notifiable Data Breaches Scheme, with specific guidance on how to meet obligations in a non-duplicative way.[32]

184. Ideally, the SPF regulators would prepare this guidance with input from the OAIC.

185. Additionally or alternatively, delegated legislation may include some of this guidance, particularly in relation to RE governance obligations. We consider this an appropriate alternative to publishing separate guidance material, particularly where mandatory controls of RE handling of information would significantly mitigate the risk of REs collecting, using and disclosing more data than is necessary.

Recommendation 1 – Develop guidance materials to support REs to comply with privacy obligations	
Issue: REs may unnecessarily collect, use and disclose more personal information than necessary to comply with their SPF obligations.	
AGS Recommendation: Unless detailed in delegated legislation, SPF regulators publish guidance materials as detailed in Annexure A.	
Response:	Noted. Treasury agrees in principle and has amended the bill to enable regulators to prepare guidance material on the framework

Conduct further PIAs for delegated legislation

186. We discuss below under APP 1.2 the requirement for an agency to conduct a PIA under the Privacy Code for 'high privacy risk' projects.

187. Various aspects of the implementation of the SPF are not within the scope of this PIA, including the implementation of delegated legislation such as SPF codes.

188. We expect the SPF codes, and potentially other delegated legislation, will provide powers to SPF sector regulators that clarify their ability to collect, use and disclose

31 See, for example, s 86G of the *Crimes Act 1914* which permits the Secretary of the Attorney General's Department to publish guidelines approved by the Information Commissioner on the operation of Part VIID.

32 In its submission, Meta raised concerns that the definition of scam to include 'obtaining personal information' as a form of harm potentially overlaps and duplicates obligations under the Privacy Act. This could potentially give rise to duplicative notification obligations to the OAIC and the SPF regulators, and require REs to send two different notifications to the same affected consumer, creating unnecessary consumer confusion and uncertainty.

personal information. This, in turn, will impact the personal information handled by REs, in particular the use and disclosure of information already held by REs for a secondary purpose. To the extent the SPF code expressly authorises the handling of this information, this may modify the operation of the APPs (by authorising under law the collection, use or disclosure of the information for new purposes).

189. Given these instruments have the ability to specify how much or how little personal information REs and SPF Regulators will handle under the SPF, we consider each instrument will comprise a 'high privacy risk' project requiring a PIA. We recommend conducting a PIA for all SPF codes and delegated legislation during the design phase.

Recommendation 2 – Complete PIA for SPF codes and delegated legislation	
Issue: Delegated legislation will contain specific detail about the powers of SPF regulators, and obligations of REs, to collect, use or disclose specific kinds of personal information. This may modify the operation of the APP by authorising the handling of personal information for new purposes.	
AGS Recommendation: An agency responsible for designing delegated legislation must conduct a PIA to comply with the Privacy Code.	
Response:	Noted. Treasury agrees in principle and will conduct PIAs where delegated legislation is likely to shape reporting requirements or impact privacy.

Require personal information to be de-identified before disclosure where possible

190. As discussed above, the SPF will result in a significant increase in the handling of personal information. Despite this, much of the personal information handled under the SPF will be ancillary to the tasks required of REs and SPF regulators under the SPF. This is because, as discussed under APP 10 below, personal information of consumers and scam victims will often be irrelevant to responding to the scam itself. Some instances may arise where this will be relevant, such as where the identity of the person who lodged a scam report is relevant to assessing the reasonableness of disruptive action.

191. Additionally, a statutory authorisation permitting disclosure will only have effect for the purposes of APP 6 where the disclosure is 'necessary' to give effect to the scheme.

192. Despite these protections, Treasury should consider expanding the SPF to pre-determine when an activity occurring under the SPF must not involve personal information. This could apply to circumstances where handling de-identified personal information would not adversely impact on the operation of the SPF. For example, Treasury could expand on proposed s 58BU to expressly clarify that personal information must be de-identified before it is disclosed for policy reasons. This would better protect against disclosing personal information where unnecessary to achieve the objects of the SPF.[33]

[33] In relation to the de-identification of unnecessary personal information, see also the concerns raised in IDCARE's submission on the exposure draft SPF.

Recommendation 3 – Consider if some SPF provisions should require de-identification	
Issue: Some provisions in the SPF permit the handling of personal information, even though it is unlikely that handling personal information will be necessary to achieve the objectives of the SPF. E.g. proposed s 58BU permits disclosure for a policy purpose when only de-identified information should be needed for this activity.	
AGS Recommendation: Treasury consider amending the draft SPF to include obligations on REs and/or SPF regulators to de-identify personal information prior to disclosure where this would not frustrate the operation of the SPF.	
Response:	Accepted. Treasury will amend the draft SPF to require de-identification of personal information where it will not frustrate the operation of the SPF.

Expand the SPF to authorise or restrict specific uses of personal information

193. REs may wish to use or disclose personal information for secondary purposes to comply with their obligations under the SPF, such as their obligation to identify higher risk consumers and their obligations to detect and disrupt scams. Secondary use of personal information may involve higher privacy risk as the individual may be unaware that their information is being used for the secondary purpose. This is why APP 6.1 affords additional protection in these circumstances.

194. Treasury could consider amending the SPF provisions to expressly authorise or restrict secondary use of personal information. Some provisions appear to impliedly authorise the secondary use of personal information however this may create uncertainty amongst REs about what the SPF does and does not authorise them to do. Alternatively, guidance materials could clarify if use of personal information is permitted, as per Recommendation 1.

195. For example, proposed s 58BK(2)(a) requires an RE to identify the 'classes' of SPF consumers of that RE who have a higher risk of being targeted by a scam. This provision does not expressly state whether REs can secondarily use customer information they already hold to carry out this task or if they should only use de-identified information.

196. It is arguable that proposed s 58BK(2)(a) fails to activate the APP 6.2(b) exception (i.e. because class identification involves identifying the characteristics of vulnerable consumers only – see [340]-[344] below). It may only authorise the use of personal information where de-identification is not possible. REs could inadvertently breach APP 6.1 by assuming this provision authorises the secondary use of identifying customer information to identify high risk classes in circumstances where this could be done on the basis of de-identified information. Increased handling of personal information also elevates the risk of other unauthorised access, use or disclosure.

197. Additionally, we consider it important to clarify how REs and SPF regulators can use personal information so as to mitigate the risk of the implementation of the SPF causing unintended consequences for SPF consumers. We identified above evidence that the UK banking sector appears to have occasionally responded to scam regulations by denying product offerings. We note also the submission on the exposure draft SPF of Bendigo Banks, which also raises this risk.

198. Restricting REs from using personal information obtained or generated under the SPF would minimise the risk of SPF consumers experiencing these unintended outcomes. For example, it may be prudent to restrict secondary use of personal information about consumers identified under s 58BK(2)(b) to protect consumers from risks such as de-banking.

Recommendation 4 – Consider altering Bill to protect vulnerable classes	
Issue: At present, it is not clear whether some provisions authorise the handling of personal information (e.g. proposed s 58BK(2)(a) is directed at identifying classes only, which could occur using aggregated or de-identified information). There is also a risk that information identifying individuals as part of a vulnerable class in proposed s 58BK(2)(b) could be used for unintended purposes, e.g. to restrict access to services.	
AGS Recommendation: In order to protect vulnerable classes, Treasury consider: • altering the bill to clarify the operation of proposed s 58BK(2) • providing clear guidance to REs on the appropriate use of personal information under proposed s 58BK(2).	
Response:	Accepted. Treasury has removed this provision from the bill.

Consider providing the SPF general regulator with a power to disclose information to overseas regulators and law enforcement agencies

199. Proposed s 58BU(2) does not contain an express power to disclose information to overseas regulators or law enforcement agencies. The ACCC submitted that this may frustrate its ability to disclose necessary information to these entities due to the protection for personal information in proposed s 58BU(3)(b).

200. We consider it would likely be reasonable, necessary and proportionate for proposed s 58BU(2) to authorise the SPF general regulator to disclose information to overseas regulators and law enforcement agencies. Scammers may reside outside of Australia and failing to include such an authorisation could significantly frustrate the SPF general regulator's ability to carry out its functions under the SPF where it is necessary to involve overseas regulators or law enforcement agencies.

201. If Treasury intend to amend proposed s 58BU to authorise this disclosure, we recommend that Treasury do so by adding a new paragraph conferring an express disclosure power into proposed s 58BU(2). We recommend that Treasury preserve the current drafting of proposed s 58BU(3)(b) such that the protection for personal information remains for information disclosures to other unregulated entities.

202. If Treasury intends to action this amendment, Treasury should also consider restricting any new authorisation to the disclosure of information to overseas regulators and law enforcement agencies. This would recognise the potential loss of control over how personal information is handled once it is disclosed overseas.

Recommendation 5 – Consider providing powers to the SPF general regulator to disclose to overseas regulators and law enforcement agencies	
Issue: In the exposure draft SPF bill, proposed s 58BU does not contain an express authorisation for the SPF general regulator to disclose information to overseas regulators and law enforcement agencies. This could frustrate the ability of the SPF general regulator to carry out its functions under the SPF because it would not be able to share personal information about suspected scammers due to proposed s 58BU(3)(b).	
AGS Recommendation: In order to enable the SPF general regulator to carry out its functions under the SPF while maximising personal privacy, Treasury consider: • altering the bill to include a new paragraph in proposed s 58BU(2) expressly authorising the SPF general regulator to disclose information to overseas regulators and law enforcement agencies • imposing restrictions on the disclosure of information to overseas regulators and law enforcement agencies, where appropriate, and • preserving the current drafting of s 58BU(3)(b) to maximise protection of personal information when disclosing to other unregulated entities.	
Response:	Accepted. Treasury will amend the bill to expressly authorise the SPF general regulator to disclose personal information to overseas regulators and law enforcement agencies, whilst preserving limitations on sharing personal information with other non-regulated entities

APP 1 – Open and transparent handling of personal information

203. The declared object of APP 1.1 is 'to ensure that APP entities manage personal information in an open and transparent way'. As the APP Guidelines recognise, management of personal information in this way not only increases accountability but can build community trust and confidence in those practices.[34]

APP 1.2 – Compliance with APPs and Privacy Code

204. APP 1.2 requires the implementation of practices, procedures and systems to ensure compliance with the APPs and any registered APP Code.

Treasury's obligations

205. Treasury, as the agency developing and administering the SPF, must satisfy the requirements of Part 2 to 4 of the Privacy Code in order to meet APP 1.2: see s 8 of the Privacy Code.

206. Part 3 of the Privacy Code includes the requirement in s 12(1) to conduct a PIA for all 'high privacy risk' projects. This term is defined in s 12(2) to encompass any changed or new way of handling personal information that are likely to have a significant impact on the privacy of individuals.

207. Implementing the SPF is a 'high risk' project. The SPF will impose many obligations on REs and SPF regulators. These entities will significantly expand how they collect, use and disclose personal information, both of scammers and victims of scams, to comply with their obligations. This expansion in the handling of personal information

[34] APP Guidelines, [1.1].

is likely to significantly impact on individuals' privacy due to the high number of entities that may handle this information and the general lack of awareness or consent by the individuals.

208. Conducting a PIA ensures that the SPF will be implemented using a 'privacy by design' approach. This includes a thorough review of the SPF provisions and development of recommendations to safeguard personal privacy.

209. This PIA must be listed in the register of PIAs kept by Treasury: Privacy Code s 15. Treasury may wish to publish this PIA, a summary version, or an edited copy, under s 13 of the Privacy Code, however any decision to release the PIA should consider the classification of the PIA.

RE obligations

210. APP 1.2 is relevant to RE governance obligations in the SPF. REs must take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. This requirement is qualified by a 'reasonable steps' test which recognises that what steps might be reasonable for an RE to take depends on circumstances such as:[35]

210.1. the nature of the information held by the RE

210.2. the possible adverse consequences for an individual if their personal information is not handled as required by the APPs

210.3. the nature of the RE, and

210.4. the practicability of taking those steps, including time and cost involved.

211. In the context of the SPF, REs will need to ensure that the governance policies, procedures, metrics and targets they develop to comply with proposed ss 58BC-58BD of the SPF comply with the requirements of APP 1.2. This means that REs will need to specifically plan for how they will meet their APP obligations when developing, implementing and revising these policies.

212. The reasonable steps test above will usually lean towards stricter privacy obligations applying to REs subject to the SPF. Many REs will handle financial or communications data, which many Australians consider sensitive. Additionally, many REs will be sophisticated entities capable of investing significant resources in privacy protection. Further, any failure to comply with the APPs may cause significant harm to SPF consumers if data is mishandled or misused.

213. The SPF provisions allow for the SPF rules to prescribe requirements and factors for RE governance policies. While the content of the SPF rules is out of scope, as per Recommendation 1, the SPF rules should require REs to prioritise protecting individual privacy when developing governance materials.

214. Additionally, as per Recommendation 1, SPF regulators should also issue guidance materials to assist REs to develop governance documents that adequately balance the need to collect sufficient personal information to comply with the SPF against the risks posed by expanding the handling of personal information.

---

35 APP Guidelines, [1.5]-[1.6].

APP 1.3 and 1.4 – Privacy policy

215. APP 1.3 requires an APP entity to have a clearly expressed and up-to-date privacy policy addressing the information detailed in APP 1.4:

Para	Requirement
APP 1.4(a)	Kinds of personal information the entity collects and holds
APP 1.4(b)	How the entity collects and holds personal information
APP 1.4(c)	The purposes for which the entity collects, holds, uses and discloses personal information
APP 1.4(d) **APP 1.4(e)**	The APP entity's privacy policy contains information about how to request access, correction or make a complaint
APP 1.4(f) **APP 1.4(g)**	Whether the APP entity is likely to disclose personal information to overseas recipients and the countries of such recipients

216. APP entities must take reasonable steps to ensure their APP privacy policy is available free of charge and in such form as is appropriate: APP 1.5. APP entities must also take reasonable steps to provide their APP privacy policy to a person or body in a particular form if requested to do so: APP 1.6.

Privacy policies, practices, procedures and systems for REs

217. REs who are subject to the APPs may need to update their privacy policy to reflect changes to how they collect, store, use and disclose personal information to comply with their SPF obligations. If Treasury decides to extend the SPF to REs that are SBOs, these REs may need to develop privacy policies, however this depends on the extent of the SBO exception.

218. This PIA does not consider the changes that REs may need to make to their privacy policies, practices, procedures and systems upon commencement of the SPF. However, to facilitate a privacy by design approach to implementing the SPF, the guidance suggested at Recommendation 1 could identify the relevant APP 1.4 matters to address in the REs privacy policy in relation to their SPF obligations.

219. In particular, this guidance could outline that REs will need to explain how they use customer personal information to prevent, disrupt and report on, and respond to, scams. This will be particularly important as individuals may not expect their personal information to be used in this way (e.g. to profile individuals at risk of scam activity), or might not understand how the handling of their personal information in this way can affect them.[36] If the RE uses automated decision-making to comply with obligations under the SPF, amendments to the Privacy Act may require the RE to include details about this use in its privacy policy.[37]

---

36 What is automated individual decision-making and profiling? | ICO

37 The Privacy and Other Legislation Amendment Bill 2024 proposes to insert an additional obligation into APP 1 to require an APP entity to provide detail in their privacy policy if the entity uses personal information in making automated decisions or substantially automated decisions that could reasonably be expected to significantly affect the rights or interests of an individual. The requirement applies if the entity has arranged for a computer program to make or do a thing that is substantially and directly related to making the decision.

Privacy policies, practices, procedures and systems of SPF regulators

220. The SPF general regulator and SPF sector regulators will collect, hold, use and disclose personal information to comply with their obligations to administer and enforce the SPF.

221. This PIA does not consider the suitability of SPF regulators' privacy policies, practices, procedures and systems. We expect that SPF regulators will need to review their privacy policies, practices, procedures and systems upon commencement of the SPF to ensure these reflect how SPF regulators will handle personal information in administering and enforcing the SPF.

Privacy policies, practices, procedures and systems for EDR scheme operators

222. This PIA does not consider the suitability of EDR scheme operators' privacy policies, practices, procedures and systems. We expect that EDR scheme operators may need to develop new policies or update existing policies to reflect their handling of personal information under the SPF. These policies should inform SPF consumers about how the EDR scheme operator will collect, use and disclose personal information.[38]

APP 2 – Anonymity and pseudonymity

223. APP 2 is intended to minimise arbitrary interference with personal privacy that can result from unnecessary requirements for individuals to identify themselves when interacting with APP entities.

224. APP 2.1 details that 'individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter'. APP 2.1 does not apply if either exception in APP 2.2 applies:

> (a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
>
> (b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Reports and complaints from consumers

225. Individual consumers will engage with REs as part of Activities 3, 4 and 5. The draft SPF provisions are largely silent on whether individuals can interact with an RE anonymously or with a pseudonym. This means that if any exception to APP 2.1 applies, it will likely be due to impracticability.

226. REs must have an 'accessible mechanism' for SPF consumers to report scams: proposed s 58BZB. This provision does not detail any requirement for consumers to identify themselves when submitting a report. It should not be impracticable for REs to accept anonymous reports as REs could create an online reporting form that does not require consumers to provide their details.

227. REs may prefer to collect personal information with consumer reports. It may assist to determine whether the report is genuine or if disruptive action is reasonable, so

[38] The existing Australian Financial Complaints Authority privacy policy may provide an example of how a privacy policy might inform consumers about how their information will be disclosed to other parties such as regulators.

as to rely on the protection of the safe harbour period. We discuss this issue further under APPs 10 and 11 below. Additionally, REs may struggle to appropriately support victims of scams to protect themselves if victims do not provide their personal information.

228. While REs may consider anonymous reports to limit their ability to prevent, detect and disrupt scams, requiring consumers to identify themselves is unlikely to be reasonable, necessary and proportionate to achieving the purposes of the SPF. The SPF is largely targeted towards combatting scams at an institutional or economy-wide scale. It is unnecessary to require consumers to identify themselves when submitting a report to meaningfully achieve the SPF's goals.[39]

229. However, in the case of SPF consumers who submit complaints for resolution through internal or external dispute resolution, it would be impracticable to remain anonymous or use a pseudonym. This is because it would be impracticable for REs or EDR scheme operators to effectively resolve an SPF consumer's complaint if the SPF consumer remains anonymous or uses a pseudonym, engaging the exception in APP 2.2(b). An SPF EDR scheme operator should aim to anonymise data where possible.

Modification of service offerings by REs to require identification

230. Some aspects of the SPF may result in REs modifying their product offerings to require SPF consumers to identify themselves when engaging with the RE. For example, an SPF sector code may require digital service providers to verify the identity of account holders.

231. The privacy impacts resulting from the SPF codes or other delegated legislation is out of scope for this PIA. However, we suggest that the relevant SPF regulator consider any APP impacts, including those related to APP 2, arising from the implementation of delegated legislation such as SPF codes (Recommendation 2).

APP 3 – Collection of personal information

232. APP 3 applies where an APP entity seeks to collect personal information, and governs those collections.

233. A collection will occur when an APP entity 'collects' the information for inclusion in a record or generally available publication: s 6 of the Privacy Act.

Kinds of personal information for collection

234. Different entities will collect a variety of kinds of personal information under the SPF. It is important to note that a 'collection' under the Privacy Act occurs not only when an APP entity first obtains the personal information about an individual, but also on each occasion the APP entity captures or records the same information within its documents or systems.

[39] Legal Aid Queensland's submission in response to the exposure legislation highlights the community's preference for having the option of anonymity where appropriate.

235. As described above at [42], personal information collected under the SPF will include that of SPF consumers, such as their name and contact details, as well as financial information.

236. Additionally, it will include personal information collected about individuals including impersonated individuals, scam perpetrators and their associates, individual who make reports and RE staff members.

APP 3.1 – Reasonably necessary or directly related to functions or activities of an agency

237. APP 3.1 provides that an agency must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the agency's functions or activities. Because of its focus on agencies, APP 3.1 will govern the collection activities of Commonwealth entities within the SPF scheme (primarily SPF regulators and government departments).

238. A collection will be 'directly related' where there is a clear and direct connection between the information for collection and the functions of the agency.

239. Whether a collection is 'reasonably necessary' for the organisation's functions and activities is an objective test, assessed from the perspective of a reasonable person who is properly informed.

240. Generally, the term 'reasonably necessary' suggests a connection that is less than essential or indispensable, but more than just helpful, or of some assistance or expedient.[40] In *Mulholland v Australian Electoral Commissioner* [2004] HCA 41 at [39], the term 'reasonably necessary' has also been equated to being 'reasonably appropriate and adapted'.

241. In *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285, Bell J noted in the context of the *Information Privacy Act 2000* (Vic) that an evaluation of whether a collection of personal information is 'reasonably necessary' should include 'balancing, in a reasonably proportionate way, the nature and importance of any legitimate purpose and the extent of the interference.' The *Jurecek* decision has since been cited with approval by the Australian Information Commissioner in interpreting APP 3.

242. A number of the activities contemplated under the SPF are likely to lead to collection of personal information by an agency. Whether these collections are permissible under APP 3.1 is determined by whether the collection is reasonably necessary for or directly related to one of its functions.

243. The key risk in relation to APP 3.1 will be overcollection of personal information which is not necessary to the administration of the SPF. The key mitigation will be identifying the kinds of information necessary for the performance of the relevant agencies' functions under the SPF and limiting collection to that information only.

Collections by the SPF general regulator

244. The functions of the SPF general regulator are set out in proposed s 58EB. Relevantly, these include 'the functions and powers of the SPF general regulator conferred by any other SPF provisions.' Consequently, where a provision of the SPF

[40] APP Guidelines at [B.113].

confers a function on the SPF general regulator which may involve the collection of personal information, APP 3.1 requires that a collection in reliance on that provision be 'reasonably necessary' for, or 'directly related' to, that function.

Collections under proposed s 58BR

245. REs will disclose personal information to the SPF general regulator under proposed s 58BR(1) (ASI reports) and proposed s 58BR(2) (scam reports). This will result in a 'collection' by the SPF general regulator. The content of these reports is set out in proposed s 58BS, which explicitly contemplates in proposed s 58BS(3) that these reports may contain the personal information of:

(a) a person reasonably suspected of committing a scam, or being knowingly involved in the commission of a scam;

(b) an SPF consumer who was engaged (or was attempted to be engaged) as part of a scam;

(c) a person who reports a scam on behalf of an SPF consumer;

(d) a person who a scam deceptively impersonates in connection with a regulated service.

Note: Personal information includes, for example, a person's name, email address, phone number, bank account details or credit card details.

246. Treasury instruct that the SPF general regulator will use these reports to disrupt[41] and prevent scams, and to enforce the SPF obligations of REs. This information may also be shared by the SPF general regulator with the operator of the SPF EDR scheme for the 'purposes of enabling or assisting the operator to perform any of the operator's functions or powers'. While we consider that some of these functions could be undertaken without using personal information contained in proposed s 58BR reports and the personal information will not be 'reasonably necessary' for these functions, such a collection will not be in excess of APP 3.1. This is because the function in disrupting scams will require the receipt of personal information, either of the victim or an impersonated person, the person reporting the scam or the perpetrator (so that it can be passed on to enforcement agencies or other REs). Personal information collected by the SPF regulator for these purposes will not be a breach of APP 3.1.

247. Ultimately, while proposed ss 58BS(2) and 58BS(3) give helpful examples of the kinds of personal information it is anticipated the SPF general regulator will require, the SPF Codes will specify the information required. Similarly, an SPF Code will specify the information required in a proposed s 58BX report.

248. A PIA of each SPF Code could review and evaluate whether the collection of specified information is reasonable, necessary and proportionate. Above as part of Recommendation 2, we have suggested conducting a PIA for each SPF Code.

Collections of reports provided under proposed s 58BX(2)

249. Relatedly, proposed s 58BX contemplates that REs will make reports to the SPF general regulator. Unlike proposed s 58BR, proposed s 58BX does not make explicit

[41] For example, the SPF general regulator may disclose 'information about a scamming action to a law enforcement agency of the Commonwealth … to assist that agency to respond to that scamming action': s 58BU(2)(d).

provision for the disclosure of personal information. We assume this provision is designed to provide oversight and accountability in relation to the surrounding provisions – particularly proposed ss 58BW and 58BZ. Additionally, Treasury instruct that the SPF general regulator may use information contained in these reports for enforcement, disruption and prevention.

250. As a consequence, given these purposes will require either the personal information of a victim or impersonated person, a person making a report or about the perpetrator, we consider it likely that the collection of personal information from proposed s 58BX reports by the SPF general regulator will in many circumstances be reasonably necessary for the SPF general regulator's disclosure functions under s 58BU.

251. However, this does not, permit the SPF general regulator to collect all personal information that may happen to be included in a record – the collection must be reasonably necessary for or directly related to one of its functions. For example, if a proposed s 58BX (or proposed s 58BR) report contained a scam report made by an SPF consumer to an RE under proposed s 58BZB, and that report contained unrelated personal information unrelated to the scam report, it would not be open to the SCG general regulator to collect it for inclusion in a record.

252. The SPF regulator will require processes to deal with unsolicited collections. We have addressed this under APP 4.

Collections under proposed s 58EF by the SPF regulators

253. Proposed s 58EF provides that an SPF regulator may disclose to another SPF regulator 'particular information or documents' or 'information or documents of a particular kind' that are 'relevant to the operation (including enforcement of the SPF provisions)'. Such a disclosure may be made by request, or at an SPF regulator's own initiative.

254. Disclosures made at an SPF regulator's initiative are dealt with below in the discussion of APP 4.1.

255. Information sharing in this way is a key measure for ensuring the success of the SPF, enabling regulators to disseminate information is necessary to detect, disrupt and prevent scams.

256. Where an SPF regulator has requested the disclosure of information or documents pursuant to s 58EF, it will have solicited that collection, and therefore will collect any related personal information in them pursuant to APP 3.1. As long as the information collected in this way by the SPF regulators is reasonably necessary or directly related to one of its own functions (either as SPF general regulator or an SPF sector regulator), it will not be in breach of APP 3.1. It will be necessary for SPF regulators, including the SPF general regulator, to ensure that it does not request disclosures containing personal information beyond its functions.

Other collections by the SPF sector regulators

257. The functions of the SPF sector regulators include those conferred by the SPF code for the sector and other SPF provisions: proposed s 58ED(3). A SPF regulator may request an RE provide a scam report under proposed s 58BR(2), in accordance with

proposed s 58BS(1). We have addressed considerations about these provisions above at [245]-[248].

258. The SPF general regulator may delegate its SPF functions to an SPF sector regulator. To the extent this occurs, a PIA may be required to ensure that the expanded collection of personal information by the SPF sector regulator is consistent with the requirements of APP 3.1 (see Recommendation 2).

Collections by Treasury/DTRDCA

259. As discussed above under Activity 1, we consider it likely that the SCF regulators will provide briefing materials to the Minister so that they can assess whether to designate a sector of the economy under proposed s 58AE.

260. Briefing materials may include historical scams data, including records about previous major scams in a sector and financial losses, to enable the Minister to assess the matters in proposed s 58AE(1)(a) and (b). While briefing materials would likely contain aggregated, de-identified data in most cases, in limited circumstances this may contain personal information if the information identifies an individual or is about an individual who is reasonably identifiable.

261. Treasury may collect historical scams information from the SPF general regulator under proposed s 58BU. This provision permits the SPF general regulator to disclose information about a scamming action where the ACCC reasonably believes that doing so will achieve the objects of the SPF as new Pt IVF of the CCA (i.e. to protect against scams as per proposed s 58AA). Proposed s 58BU will be conditioned by a requirement of 'reasonable belief' that doing so will assist in achieving the objects of the SPF. We note that, in this context, sharing personal information, unless de-identified, is unlikely to assist in achieving these objects, given Treasury could develop or administer SPF-related policy using de-identified information. We are in any case instructed that Treasury is unlikely to ever request personal information in this context, and presently receives macro-level reporting from the ACCC on scam trends.

262. Additionally, Treasury may obtain information from other sources, such as open source information, to inform a brief. This is unlikely to include personal information.

263. In summary, we consider that collecting personal information in an identifiable form is unlikely to be reasonably necessary for or directly related to the Minister's functions in designating a sector, and thereby a breach of APP 3.1 (Recommendation 3 suggests relevant amendments to ensure the provision does not unnecessarily authorise the sharing of personal information for a policy purpose). However, if the SPF general regulator discloses de-identified information only in accordance with proposed s 58BU, we think the requirement in APP 3.1 will be met.

APP 3.2 – Reasonably necessary for functions of an organisation

264. APP 3.2 provides that an organisation that is an APP entity must not collect personal information unless the information is reasonably necessary for one or more of the organisations functions or activities.

265. The SPF will require REs, which are organisations and thereby subject to APP 3.2 rather than 3.1, to collect personal information in order to prevent scams (Activity 3),

as well as detect, disrupt, report and respond to scams (see Activity 4). Stopping customers falling victim to scams is very likely a function of REs at present, and will plainly be a function of REs following the introduction of the SPF, which imposes this function upon them. REs will consequently be authorised to collect personal information (such as through the receipt of scam reports from SPF consumers pursuant to proposed s 58BZB).

266. A key risk, however, will be that REs over-collect information that is unnecessary for the performance of this, or their other, functions. For example, in the creation of a mechanism to easily report scams pursuant to s 58BZB, REs should ensure that they are not soliciting information going beyond that necessary to fulfil their SPF functions.

267. To assist REs with developing privacy enhancing mechanisms to report scams, we suggest the SPF general regulator publish guidance materials, e.g. which may give examples of template reports or the kinds of information an RE should usually obtain to facilitate reporting under proposed s 58BR (Recommendation 1).

268. To the extent that a sector-specific SPF code made under s 58CB will impose different requirements around collection for REs in that sector, we recommend conducting a separate PIA on that code (Recommendation 2).

APP 3.3 and APP 3.4 – collection of sensitive information

269. APP 3.3 states that an APP entity must not collect sensitive information unless:

269.1. the APP entity is an agency and the sensitive information is reasonably necessary for or directly related to the agency's functions or activities (as required by APP 3.1) and the individual consents to the collection; or

269.2. the APP entity is an organisation and the sensitive information is reasonably necessary for the agency's functions or activities (as required by APP 3.1) and the individual consents to the collection; or

269.3. an exception in APP 3.4 applies in relation to that information.

270. Sensitive information is defined in s 6(1) of the Privacy Act (see the Glossary to this PIA).

271. We consider it fairly unlikely that REs and SPF regulators will collect sensitive information frequently as part of the SPF. However, to the extent that a scam attempts to take advantage of a potential victim's membership of, for example, a particular religious or ethnic group, and information collected by an RE or SPF regulator discloses that membership, it will be necessary for APP 3.3 and 3.4 to be complied with.

Collection of sensitive information by REs

272. In cases where an individual voluntarily discloses their affiliation as part of a report made to an RE under proposed s 58BZB, they will have relevantly consented to the collection of that information under APP 3.3.

273. In other cases, such as where an RE collects sensitive information through their own investigations, it will be necessary for that RE to comply with a relevant APP 3.4 exception. The most relevant exception is likely to be APP 3.4(a):

Exception	Requirement
APP 3.4(a)	The collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

274. A collection may be 'required or authorised by or under' a law even if it is not directly provided for by the law.[42] A 'requirement or authorisation to divulge personal information may also arise by necessary implication from a law that is directed to a purpose other than the disclosure of records or information'.[43] APP 3.4(a) does not, however, 'extend to authoris[ing] any disclosure that is merely incidental, convenient or conducive to the fulfilment of some other statutory obligation. ... The critical factor is the necessity of drawing the relevant implication in order to give effect to the statutory scheme or, alternatively, to avoid frustrating the statutory scheme.'[44]

275. Proposed s 58BS(2) provides that the SPF general regulator may prescribe the kinds of information which *must* be included in a s 58BR report. A note to sub-s (2) provides that this may include 'de-identified demographical information about the impact SPF consumer'. We consider that this impliedly authorises the *collection* of demographic information (which may include sensitive information) by the RE for the purposes of the APP 3.4(a) exception, in the sense that the permissibility of the collection of that information is a necessary implication.

276. That information will be personal information at the time of the collection, given it is attributable to an identified person, even if it is later de-identified. Consequently, depending on the content of the notifiable instrument ultimately made under proposed s 58BS, this will provide a valid basis for the collection of sensitive information by REs, where it is required to be provided under a relevant report.

Collection of sensitive information by SPF regulators

277. There are two likely means by which SPF regulators may collect personal information: where they receive it from REs as part of reporting requirements, and where it is passed to them by other SPF regulators under proposed s 58EF.

278. As above, where the information is divulged through a proposed s 58BZB report before being reported to an SPF regulator, the reporting individual will have consented, as long as the proposed s 58BZB reporting mechanism clearly obtains valid consenting to share the report with the relevant regulators). While consent is best practice, where there is an obligation to pass the report to an SPF regulator, the RE will not require consent to make the disclosure. Additionally, there may well be personal information of individuals other than the reporter contained in the report.

279. In these circumstances, or where an RE has otherwise obtained the information through its own investigations before reporting it to a regulator, and consent for the SPF regulator to collect it has not been obtained from the individual concerned, it will be necessary to engage an APP 3.4 exception. The same will be true where an SPF regulator collects information provided by another SPF regulator under proposed s 58EF.

---

42 ***AIT18*** *v Australian Information Commissioner* [2018] FCAFC 192 at [123], a decision relating to the comparable Information Privacy Principle 11 (now repealed).

43 *AIT18* at [125].

44 *AIT18* at [129].

280. In relation to proposed s 58EF collections, we consider that APP 3.4(a) will likely be engaged here, meaning that sensitive information may be collected by SPF regulators where it is 'relevant to the operation (including enforcement) of the SPF provisions'. While only *disclosure* is authorised on face of provision itself, we consider proposed s 58EF to impliedly authorise a collection as a necessary corollary of the disclosure.

281. APP 3.4(a) may also be engaged if proposed s 58BR requires sensitive information to be provided in a form that connects it to an identifiable individual, rather than in the form of deidentified demographic data as presently contemplated in the note to the section.

APP 3.5 – Fair and lawful means

282. APP 3.5 provides that APP entities must collect personal information only by lawful and fair means.

283. 'Lawful means' are any method that is not criminal, illegal, prohibited or proscribed by legislation: APP Guidelines at [3.60]-[3.61].

284. 'Fair means' are methods of collecting information that do not involve intimidation or deception, and are not unreasonably intrusive: APP Guidelines at [3.62].

285. We are not aware of any contemplated modes of collection that are unlawful. We also do not think that the SPF is likely to involve collection in ways that are unfair.

286. However, it will be important for REs to explain how they are collecting information, and for what purposes, to ensure individuals are informed as to how their information will be used (see further below the discussion under APP 5). That an individual is informed of the nature and purposes of a collection may influence its fairness.

287. Above, at paragraph [198] we noted denial of service or debanking risks, informed by the UK experience. If REs begin to collect data in underhanded or deceptive ways, and use that data to decide to deny service to an individual on the basis that they pose an unacceptable scam risk, or wish to avoid any SPF obligations that may otherwise arise, this may raise the greatest risk of an 'unfair' collection related to the scheme.

288. We also consider that the purpose for which a collection is made may influence whether or not it is fair. Where SPF regulators or REs seek to collect information pursuant to statutory obligations to protect SPF consumers, the collection is likely to be fair within that context.

APP 3.6 – Collection from another individual

289. APP 3.6 requires an APP entity to collect personal information directly from an individual unless one of the following exceptions applies:

Exception	Requirement
APP 3.6(a)(i)	*For agencies only* - the individual consents to the collection from the third party
APP 3.6(a)(ii)	*For agencies only* - the collection from a third party is required or authorised by or under an Australian law or Court or Tribunal order

APP 3.6(b)	It is unreasonable or impracticable to collect the information directly from the individual.

Indirect collections by SPF regulators

290. We repeat our observations above in relation to the circumstances in which APP 3.4(a) authorises collection of sensitive information, as this applies equally to indirect collection through the APP 3.6(a)(ii) exception. This will cover, among other things, proposed s 58EF collections from other SPF regulators which are relevantly required or authorised under a law.

291. Beyond this, we consider that it will generally be impracticable or unreasonable (for APP 3.6(b) purposes) for SPF regulators to obtain information they receive from REs from the individual concerned directly.[45] This is in large part because the SPF regulator will not know what the information is before they receive it, nor will they likely have contact details for the individual concerned, and speed may well be of the essence in responding. There are also further policy considerations tending towards the impracticality of direct collection: receiving reports from REs directly will avoid double handling of information as well as standardising reporting and improving its quality; it helps ensure that REs are aware of scam activity without waiting to be notified by the SPF regulators; and the REs may be able to provide further useful information alongside reports that consumers do not have. In any event, as most collections will be expressly or impliedly authorised by a law for APP 3.6(a)(ii) purposes, it is unlikely that this provision will need to be relied on.

292. We also understand that it is possible that SPF regulators may undertake their own open source investigations of scam activities. While it is difficult to provide advice on these collections in the abstract, we think it unlikely that they will contain personal information and, as a very broad proposition, if these collections do contain personal information it is likely that it will be unreasonable or impracticable to obtain this information from the individuals concerned. It may be appropriate to include something to this effect in any guidelines to SPF regulators.

Indirect collections by REs

293. Under the SPF, REs will collect a large amount of personal information directly from the individual concerned. In some circumstances, such as where a proposed s 58BZB report contains personal information of a scammer, or where the RE collects information as in the course of an investigation it has conducted, it may collect information indirectly. This collection is very likely to be required or authorised under a law for APP 3.6.(a)(ii) purposes – either proposed s 58BZB, or else proposed s 58BW.

294. It is also likely, although in most cases unnecessary to rely on, that personal information collected in the course of an investigation, whether it belongs to a scammer or an SPF consumer, is unreasonable or impracticable to collect directly from an individual. In the case of an SPF consumer, it will be impracticable for the information to be collected directly from the individual because the RE will not be aware what the information is, and therefore will not be able to ask for it, before it

[45] Noting, however, that the ACCC will still receive some reports on scam activity directly from the individuals concerned through the Scamwatch program.

commences investigating. In the case of a scammer, it will be unreasonable because it would tip the scammer off to the investigatory activity of the RE.

APP 4 – Unsolicited personal information

295. APP 4.1 requires that if an APP entity receives personal information, and the entity did not solicit the information, the entity must, within a reasonable period after receiving the information, determine whether the entity could have collected the information under APP 3 if the entity had solicited the information.

296. If it is not personal information that could be collected under APP 3, the APP entity must destroy or deidentify it.

Receipt of unsolicited personal information by REs

297. We consider the probability of REs receiving unsolicited personal information to be low. Perhaps some information may be received through proposed s 58BZB scam reports that is not related to a scam attempt – if so, assuming the information is not of a kind that could be lawfully collected under APP 3.2 (ie, it is not reasonably necessary for one or more of the RE's functions or activities), then it should be destroyed or deidentified pursuant to APP 4.3.

298. SPF regulators could publish guidance on this obligation, and potential de-identification methods in materials published as per Recommendation 1.

Receipt of unsolicited personal information by SPF regulators

299. SPF regulators are at risk of receiving unsolicited personal information from two main sources: REs providing reports under proposed ss 58BR and 58BX, and other SPF regulators sharing information under proposed s 58EF.

300. We consider that this risk of overprovision of information can be effectively mitigated by clear guidance to REs, whether in statute, delegated legislation or guidelines (Recommendation 1), about what information should be contained in the reports. Where information is required to be provided to an SPF regulator, it will not be unsolicited.

301. As noted above, information may be provided under proposed s 58EF either on request of a receiving regulator or at the initiative of the providing regulator. Where unsolicited personal information is provided by one SPF regulator to another, the receiving regulator should consider whether they would be entitled to collect it under APP 3.1, as outlined above. If the SPF regulator cannot collect the information, it will need to consider how it can handle the information in accordance with its usual record keeping practices, including any normal administrative practice to destroy irrelevant and low value information.

APP 5 – Notice of collection

302. APP 5 provides that:

> At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:
>
> (a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or
>
> (b) to otherwise ensure that the individual is aware of any such matters.

303. The matters referred to in APP 5.2 are set out in the table below.

Para	Description
APP 5.2(a)	Identity and contact information for APP entity
APP 5.2(b)	Advise of any third-party collection
APP 5.2(c)	State if the collection required or authorised by or under law
APP 5.2(d)	State the purpose of collection
APP 5.2(e)	The main consequences (if any) if the information is not collected
APP 5.2(f)	Details of any usual disclosures
APP 5.2(g) **APP 5.2(h)**	The APP entity's privacy policy contains information about how to request access, correction or make a complaint
APP 5.2(i) **APP 5.2(j)**	Whether the APP entity is likely to disclose personal information to overseas recipients and the countries of such recipients

304. All relevant APP entities, both REs and SPF regulators, should ensure that they provide appropriate notification of their collection activities, including through updating their privacy policies and providing guidance materials on their website about their SPF activities more broadly.

305. We suggest that REs inform SPF consumers of the uses their personal information may be put to within the SPF scheme at the time of collection, where collection is carried out directly. Additionally, if an RE collects personal information indirectly, such as through investigations of scam activity, they should update information on their website, such as a privacy policy, to ensure that relevant information is provided (Recommendation 1).[46] Notice of this kind will be important given the broad definition of 'SPF consumer' in proposed s 58AH(1) which will extend beyond current customers to potential RE customers.[47]

306. SPF regulators will carry out indirect collection, as discussed above. Similarly, those regulators should ensure that their privacy policies notify the relevant APP 5.2 matters to individuals whose personal information may be indirectly collected by the SPF regulators.

---

46 See the observations of the Information Commissioner in *'RC' and TICA Default Tenancy Control Pty Ltd (Privacy)* [2019] AICmr 60 at [78], which suggest that it may be reasonable to notify a class of individuals (rather than a specific individual) of the actual or potential collection of their personal information, including by providing a notice on the APP entity's website.

47 See submission from Customer Owned Banking Association which expressed concern as to how its members would provide notice of collection to non-customers.

307. We have considered, in this context, the effect of proposed s 58EH, which provides that an SPF regulator need not notify any person that it:

307.1. plans to make a disclosure under proposed s 58EF

307.2. has made such a disclosure

307.3. plans to use information or documents disclosed under proposed s 58EF

307.4. has used information or documents so disclosed.

308. We note that, while this section relieves SPF regulators of possible obligations in relation to notification of *disclosure* or *use*, we do not think it relieves the SPF regulators of the obligation to provide notice of collections. However, this obligation is unlikely to be onerous in circumstances where, in most cases, it will be sufficient to provide notice on the SPF regulator's website that it undertakes such collections.

309. Additionally, we think providing notice of this kind is consistent with providing transparency about the handling of personal information by SPF regulators, to enable individuals to exercise privacy rights in relation to the handling of their personal information (see APPs 12-13).

310. We also note IDCARE's submissions on the exposure draft to the effect that consumers should receive notice and give consent before their personal information is disclosed or used by SPF regulators and law enforcement. We consider that the exposure draft SPF strikes a reasonable balance between the desirability of individuals having awareness of the handling of their personal information and the need for SPF regulators to act quickly as:

310.1. obtaining consent from relevant individuals may delay a response to a scam, increasing the harm caused to consumers

310.2. providing notifications may tip off scammers, who can alter their behaviour to avoid detection and/or prosecution.

311. We note also that there is nothing in the exposure draft SPF which prevents REs and SPF regulators providing notifications to consumers of the use of their personal information, and we agree with IDCARE that there are some circumstances in which it will be appropriate to do so. For example, where certain protective action is taken in relation to a consumer who is at risk of falling victim to a scam, like reports to Credit Reporting Bodies or temporary freezing of accounts, it will generally be appropriate to notify these actions.

312. We suggest providing guidance to REs on the circumstances in which reasonable steps would require notification of the handling of their personal information under the SPF (Recommendation 1).

APP 6 – Use or disclosure of personal information

313. APP 6 provides that an APP entity can only use or disclose personal information for the purpose for which it was collected (the 'primary purpose'), or for a secondary purpose if the individual has consented to the use or disclosure, or an exception applies. The relevant exception is:

Exception	Description
APP 6.2(b)	The use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order

Uses and disclosures by SPF regulators

314. Activities 4 and 6 will involve the use of personal information by SPF regulators received in reports to detect, disrupt and respond to scams.

315. Activities 1, 5-8 will involves the disclosure of personal information by SPF regulators.

Disclosure by SPF general regulator to Treasury /disclosure to the Minister

316. Activity 1 potentially involves the disclosure by the SPF general regulator to Treasury, and from them to the Minister. As discussed above at [261], we think it unlikely any disclosure of personal information will occur as the SPF general regulator will not 'reasonably believe' the data will assist Treasury to develop or administer policy related to the SPF. Nor is personal information likely to assist the Minister in designating a sector under proposed s 58AC.

Use and disclosure by SPF regulators of scam reports and other personal information for the purpose of the SPF framework

317. Generally, an SPF regulator will use and disclosure personal information the entity receives under the SPF for the same purpose for which it collected the information (i.e. to detect, disrupt and respond to scam activity). As the use will occur for the primary collection purpose, APP 6.1 will be met.

318. However, because some of the SPF regulators are subject to protected information provisions with their own legislation, specific authorisations to disclose information are required. Similarly, if the use or disclosure occurs for a secondary purpose, a specific statutory authorisation may be necessary due to equitable or statutory obligations of confidence.[48]

319. We have set out below a summary of the relevant provisions.

Legislation	Summary of provisions
Competition and Consumer Act 2010, s 1555AAA(1)(b)(i)	A Commission official must not disclose protected information[49] to any person except when the Commission official or the Commission is required or permitted by any other law of the Commonwealth.
Australian Communications and Media Authority Act 2005 (**ACMA**	The exposure draft SPF Bill includes proposed s 59DB which will permit an ACMA official authorised

[48] *Johns v Australian Securities Commission* (1993) 178 CLR 408, 424 (Brennan J).

[49] 'Protected information' relevantly means information that was given in confidence to the ACCC under proposed Pt IVF (as a core statutory provision).

Legislation	Summary of provisions
Act), proposed s 59DB to the draft SPF bill	by the Chair to disclose 'authorised disclosure information'[50] to either an SPF regulator or an operator of an SPF EDR scheme for the purposes of the SPF.
Australian Securities and Investments Commission Act 2001 (**ASIC Act**), ss 127(1), 127(2)	ASIC must take all reasonable steps to protect protected information,[51] and information given to it confidence in or in connection with the performance of its powers under the corporations legislation from use or disclosure, except whether required or permitted by a law of the Commonwealth.

320. There are 3 specific provisions which authorise disclosures in certain circumstances. Each of these disclosures, where validly authorised, will fall within the APP 6.2(b) exception.

Proposed s 58EF disclosures between SPF regulators

321. Proposed s 58EF establishes a scheme for SPF regulators to disclose information to each other (Activity 7). The note to this provision states that proposed s 58EF will act as an authorisation for s 155AAA(1)(b) of the Competition and Consumer Act, proposed s 59DB of the ACMA Act and s 127(2) of the ASIC Act.

Proposed s 58BU disclosures by SPF general regulator

322. Proposed s 58BU confers a power on the SPF general regulator to disclose information about a scam if it 'reasonably believes that doing so will assist in achieving the object of this Part' (Activity 4, Activity 6). The proposed provision is broad – it authorises disclosing information in a wide variety of circumstances, including to assist in developing policy, to assist in disrupting specific scam actions, and to assist in disrupting other similar actions.

323. It is clear from the text and structure of the provision that it contemplates the disclosure of personal information – see proposed s 58BU(3) which specifically *prohibits* the sharing of personal information in a specific context. It can be inferred that personal information is permitted in other contexts subject to the caveat below.

324. As discussed above at [261], proposed s 58BU only authorises disclosures where the SPF general regulator '*reasonably believes that doing so will assist in achieving the object of the SPF'*. In other words, the SPF general regulator can only disclose information (including personal information) under the provision where doing so will assist in achieving the object of the relevant Part of the Act. For example, the SPF general regulator could share a scammer's name where the ACCC reasonably believes the disclosure will assist a law enforcement agency to respond to the scamming action: see proposed s 58BU(2)(d).

---

50 'Authorised disclosure information' relevantly means (a) information given in confidence to ACMA in connection with the performance of any of ACMA's functions or the exercise of any of its powers, or (c) information obtained by ACMA as a result of the exercise of powers under a provision that allows ACMA to require a person to give information or produce a document: ACMA Act, s 3.

51 'Protected Information' means information disclosed or obtained, or a document given or produced, that relates to the affairs of a person regulated by ASIC, or a person who has been, is, or proposed to be a customer of a body or person related by ASIC: ASIC Act, s 127(9).

325. We are instructed that the SPF general regulator will disclose information such as, for example, the numbers of bank accounts associated with suspected scam activity. If the identity of the scammer is not known by the ACCC, but the information could be used by the recipient to determine the identity of the scammer, it will constitute personal information (as it will relate to a reasonably identifiable person). Even if the identity of the scammer cannot be reasonably identifiable, proposed s 58BU will authorise that disclosure for the purposes of APP 6.2(b).

Disclosure by SPF regulators to the operator of an EDR scheme

326. Proposed s 58DE contemplates the SPF regulators disclosing information to the operator of an SPF EDR scheme for the sector 'for the purposes of enabling or assisting the operator to perform any of the operator's functions or powers'. As with all statutory provisions, the power of disclosure in s 58DE will be conditioned by a requirement of reasonableness. This means that proposed s 58DE will permit the information reasonably required by the SPF EDR operator to perform their functions or powers, but not information in addition to this. This is consistent with APP 10.2 which requires APP entities to take reasonable steps to disclose 'relevant' personal information.

Uses and disclosures by REs

327. Activities 2-5 will involve the use and disclosure of personal information by REs.

328. Where REs use and disclose personal information collected a scam prevention purpose (e.g. in consumer reports) for the same purpose, the use and disclosure will comply with APP 6.1. This may include disclosing information about actual scammers to affected consumers to respond to a scam.[52] Given notifying consumers may unintentionally disclose details about scam detection methods, REs may benefit from guidance on how to comply with reporting obligations without compromising efforts to prevent, disrupt and respond to scams (Recommendation 1).[53]

329. However, REs will also use and disclose existing personal information collected to provide services to its customers for secondary purposes to meet SPF obligations.

330. We discuss below the three circumstances in which these disclosures are required or authorised by or under law, engaging the exception in APP 6.2(b).

Disclosures by REs to SPF regulators to detect, disrupt and respond to scams under proposed ss 58BR and reporting on scams under 58BX

331. Disclosures of personal information contained in reports under proposed ss 58BR and 58BX will be required or authorised by law if the personal information is of a kind ultimately specified by the SPF general regulator by notifiable instrument under ss 58BS(2) and 58BX(4).[54] While the collection and dissemination of information by

---

52 The submissions from Legal Aid Queensland and the Consumer Action Law Centre emphasised the importance of REs having the ability to provide the personal information of scammers directly to individuals to enable them to respond to the scam (e.g. take legal action against them).

53 See the submission from the Australian Mobile Telecommunications Association.

54 Notwithstanding that the types of information to be reported will be prescribed by notifiable instrument rather than delegated legislation, this will constitute an authorisation or

SPF regulators is a key part of the SPF framework, we think a PIA will be required to determine whether the collection of specific information under the notifiable instrument is reasonable, necessary and proportionate in the circumstances (Recommendation 2).

332. Additionally, REs will need to take care not to overreport information within these reports, and/or provide information because it might be useful or of assistance. Disclosures of this type risk non-compliance with APP 3.1 by the SPF regulators: see *'WL' and Secretary to the Department of Defence* [2020] AICmr 69 at [99]-[100].

333. We recommend providing guidance to REs on the information reporting requirements to ensure REs provide only necessary information (Recommendation 1).

Secondary use of personal information by REs to develop policies and procedures

334. Subdivision C of the bill sets out a variety of governance obligations of REs. In particular, proposed s 58BD sets out particular topic to be covered by governance policies, which must be developed by reference to factors including the kinds of SPF consumers of its regulated services, and any other relevant factors.

335. There is some risk that in developing these policies, and particularly in determining the 'kinds of SPF consumers' of the regulated services, a secondary use may be made of personal information collected by REs, either as part of scam reports, or their regular service delivery activities. If this occurs, the use may not be 'necessary' to give effect to the statutory scheme[55], so that the use is covered by APP 6.2(b).

336. To minimise the risk of breaching APP 6 in developing governance policies, we recommend the SPF general regular issue guidance about the kind of activities required to meet the obligations under proposed s 58BD, and how REs can conduct these activities using aggregated or de-identified personal information (Recommendation 1).

Secondary use of customer information by REs to disrupt scams

337. Proposed s 58BW imposes an obligation on REs to take steps to disrupt scams relating to ASI held by the entity. In so doing, it seems likely that REs may wish to use other personal information held by the RE for a secondary purpose. For example, a user of a service may have provided an email address or phone number and specified its use in relation to specific types of communication. The RE may wish to use the email address or phone number to contact them to warn them of the scam.

338. Where the use or disclosure of personal information for a secondary purpose is necessary to disrupt a scam or suspected scam, we think proposed s 58BW will impliedly require the use or disclosure to avoid frustration of the statutory scheme.[56]

339. Nevertheless, we consider it prudent that REs notify their customers at the point of collection of personal information that it also collects their personal information to

---

requirement 'by an Australian law' since the SPF itself compels that the notifiable instrument be complied with.

55 *AIT18 v Australian Information Commissioner* [2018] FCAFC 192 at [122]-[129].

56 *AIT18 v Australian Information Commissioner* [2018] FCAFC 192 at [122]-[129].

prevent, detect or disrupt scams. Where collection genuinely occurs for an SPF purpose, the prohibition in APP 6.1 will not apply.

Secondary use of customer information by REs to identify and warn higher-risk classes of SPF consumers – s 58BK(2)

340. Under s 58BK(2), as discussed above at paragraph [90] and [195], REs are required to identify the classes of SPF consumers of that entity who have a higher risk of being targeted by a scam (**vulnerable classes**). Section 58BK itself offers little guidance as to how REs should identify vulnerable classes, but some guidance is provided by the EM at [1.134] which contemplates that REs:

340.1. 'may identify consumers who are at higher risk based on how they use its service, or due to other factors',

340.2. 'may also identify vulnerable cohorts of consumers with reference to information it receives from scam reports or public reports released by the SPF general regulator', and

340.3. 'may identify consumers from a particular geographic location or age cohort are subject to an increase in scam activity on its service'.

341. Unless REs capture this sort of demographic scam data in a deidentified form, this analysis is **highly likely** to involve a use of personal information for a secondary purpose.

342. For example, REs may use birthdates, collected for identification purposes, to analyse the ages of SPF consumers who fall victim to scams to determine whether older customers have a higher risk of being targeted for the purposes of proposed s 58BK(2)(a).

343. Unless deidentification of the data is not possible, we consider it likely that secondary use of personal information for a proposed s 58BK(2)(a) purpose will breach APP 6. This is because such a use appears unlikely, at least in many cases, to be 'reasonably expected' by individuals to an extent capable of engaging the APP 6.2(a) exception. It is also likely, in cases such as that identified above, not to 'directly relate' to the primary purpose for which the information was collected. Further, in circumstances relating to the *prevention* rather than disruption of scams, a permitted general situation is unlikely to exist.

344. As a consequence, the only possible exception is APP 6.2(b). However, while analysis of personal information of scam victims appears to be a sensible way of complying with the proposed s 58BK(2) requirement, the subsection appears not to generally *require* such an analysis, as discussed at paragraph [196] above. For example, an RE could conduct the analysis by examining trends based on consumers within a 5 year age bracket. Only where deidentification is not possible, would an implied requirement or authorisation exist.

345. However, the RE will need to use personal information to identify which customers they need to provide warnings to for the purposes of proposed s 58BK(2)(b). This secondary use of personal information – to identify which consumers falls within a vulnerable class and therefore should be warned – appears to be impliedly contemplated by proposed s 58BK(2)(b), and will therefore fall within the APP 6.2(b)

exception. This stands in contrast to the original analysis to identify vulnerable classes.

346. As it presently stands, the task of identifying vulnerable classes and then notifying them will need to be conducted in two stages in order to comply with APP 6. Generally, deidentified data will need to be used to determine the vulnerable classes, before the personal information of individuals is used to identify them as falling within a particular class. For example, the RE might keep a database of deidentified demographic data (such as age) of individuals who have made scam reports. Once the RE has analysed this data and identified a vulnerable class, the RE must notify SCF customers within that class. By contrast, the analysis of a single database containing customer name and demographic characteristics, as well as a field indicating whether the customer had lodged a scam report, would breach APP 6.[57]

347. To ensure REs are clear that the obligation in proposed s 58BK(2)(a) will not require the use of personal information, Treasury could consider adding a note to make clear that REs should use deidentified or aggregated data, unless this is not possible (see Recommendation 4). This should also be the subject of RE guidance (Recommendation 1).

APP 7 – Direct marketing

348. This APP is not relevant to the SPF, as it is not envisioned that REs or SPF regulators will use personal information collected under the SPF for the purpose of direct marketing. However, REs are likely to collect additional information under the SPF that could be inappropriately used for direct marketing. The Legal Aid Queensland's submission in response to the exposure legislation expressly raises this issue.

349. Importantly, we do not consider that any of the exceptions under APP 7 will apply to information collected under the SPF such that the restriction in APP 7.1 will apply to REs. We suggest providing guidance on this point to REs for the avoidance of doubt (Recommendation 1).

APP 8 – Cross-border disclosure of personal information

350. APP 8.1 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information.

351. Under s 16C of the Privacy Act, where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs.

352. APP 8.1 does not apply where an exception in APP 8.2 exists, relevantly:

[57] Similarly, the example of cryptocurrency users at paragraph [**Error! Reference source not found.**] above might involve use of personal information (bank transactions) to identify a higher-risk class.

Exception	Description
APP 8.2(c)	APP 8.1 does not apply in circumstances where the disclosure of information is required or authorised by an Australian law.

353. The SPF is intended to capture Australian SPF consumers residing outside of Australia and some REs may be multinational companies located outside Australia. REs and SPF regulators may therefore need to disclose personal information to an overseas recipient to comply with their obligations under the SPF.

354. REs may need to disclose personal information to Australian SPF consumers who are residing overseas. For example, an RE may need to disclose an SPF consumer's personal information to a SPF consumer living overseas so that the SPF consumer can participate in an internal dispute resolution process. APP 8.1. does not apply to a cross-border disclosure made to the individual themselves.

355. Some REs subject to the SPF may not be resident in Australia. This means that the SPF general regulator may disclose personal information overseas where it shares personal information to a foreign-resident RE, for example under proposed s 58BU. This includes disclosure of personal information of victims of scams and scam perpetrators.

356. However, APP 8.1 will not apply where disclosure of personal information is necessary to give effect to a provision in the SPF. In other words, where the SPF regulator can only comply with proposed s 58BU by disclosing personal information about a scam victim or perpetrator, the disclosure will be impliedly authorised by law, satisfying APP 8.2(c).

357. We consider it reasonable, necessary and proportionate for REs and SPF regulators to disclose information to overseas recipients. Many Australians rely on products provided by foreign-based REs and many Australians residing overseas continue to access Australian products, such as holding an Australian bank account. Prohibiting cross-border disclosure of personal information would frustrate the SPF and create a loophole where scammers could target foreign-based REs to avoid detection and disruption of their scam under the SPF.

Disclosure to overseas regulators and law enforcement agencies

358. In the event that Treasury intends to amend proposed s 58BU in response to the ACCC's submission on the exposure draft legislation (see [199]-[202] above), per Recommendation 5, by inserting a new express authorisation permitting disclosure to overseas regulators and law enforcement agencies, this would activate the exception at APP 8.2(c).

APP 9 – Adoption, use or disclosure of government related identifiers

359. This APP is not relevant to the SPF, as it is not envisioned that REs or SPF regulators will adopt, use or disclose government related identifiers.

APP 10 – Quality of personal information

360. APP 10 has two limbs directed at ensuring the integrity of the personal information handled by REs and SPF regulators.

APP 10	Description
APP 10.1 – Collection	Such steps as are reasonable in the circumstances to ensure that the personal information it collects is accurate, up-to-date and complete.
APP 10.2 – Use / Disclosure	Such steps as are reasonable in the circumstances to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

361. According to the APP Guidelines at 10.12-10.19, personal information is:

361.1. **inaccurate** if it contains an error or defect, or if it is misleading

361.2. **out-of-date** if it contains facts or opinions that are no longer current

361.3. **incomplete** if it presents a partial or misleading picture

361.4. **irrelevant** if it does not have a bearing or connection to the purpose of the use or disclosure.

362. The SPF does not impose any specific obligations on REs or SPF regulators to ensure the quality of personal information of consumers who report scams. However, the 'reasonable steps' in APP 10 will be relevant to assessing if an RE has acted reasonably, as required by some provisions in the SPF.

Scam victims and consumers

Collection of personal information

363. As discussed at APP 2, we consider that SPF consumers should be able to make reports anonymously as it is unnecessary for an RE to confirm the identity of the person making a report to assess or act on the report. Therefore, REs will only need to take limited steps to comply with APP 10.1 when collecting consumer reports.

Use and disclosure of personal information

364. REs will need to comply with a higher standard of reasonableness to use and disclose personal information of scam victims and consumers. A higher standard of reasonableness is proportionate because of the risk of harm to consumers if REs act on inaccurate, out-of-date or incomplete information. For example, an RE may cause significant detriment to a consumer if it takes disruptive action under proposed s 58BW in relation to a bank account that is not actually being used to conduct scams.

365. This risk is best demonstrated by the case of anonymous lodgement of malicious reports. For example, an entity could lodge an anonymous report against a competitor in an attempt to have the competitor's social media page blocked by an RE through disruptive action.

366. REs will likely need to review reports received from scam victims and consumers against their customer records to verify its authenticity and to establish whether the RE needs to investigate further. We consider this obligation is captured in the current drafting of the SPF as most provisions require an RE to act reasonably.

367. For example, proposed s 58BW requires an RE to take reasonable steps to disrupt a scam. While it may be unreasonable for an RE to block a social media page due

to a single anonymous scam report, it could be reasonable for the RE to block the social media page if it receives a number of detailed reports about the same social media page.

368. However, we think providing guidance to REs on what might be 'reasonable steps' to take in particular circumstances would assist REs to comply with their obligations under APP 10 (as per Recommendation 1). This guidance could provide examples of how an RE might act in a range of scenarios where REs have different levels of information.

Scammers

369. The SPF also does not contain specific obligations on REs or SPF regulators to ensure the quality of personal information regarding scammers who are the subject of ASI and scam reports. While the case is stronger to impose obligations to ensure the quality of personal information, such as to ensure a telephone number belongs to a specific scammer, we consider this risk is also mitigated by the standard of reasonableness present throughout the SPF.

370. As discussed above, REs will be expected to tailor how they act on scam reports and ASI based on the quality of the information they hold. An RE will only receive the benefit of safe harbour protection under proposed s 58BZ if the action it takes is reasonably proportionate to the suspected scam and the information that would reasonably be expected to be available to the RE. It may not be reasonably proportionate for an RE to take action such as blocking social media pages and phone numbers if it is unsure about whether the scammer owns and is using these channels.

371. It is also unlikely to be reasonable to impose obligations on REs to verify the personal information of scammers before using or disclosing this information. REs and scam victims are subject to extreme information asymmetry and may not know or have any way of ascertaining key information about a scammer. Imposing obligations on REs to verify this information, beyond the existing standard of reasonableness, risks frustrating the SPF by restricting the ability of REs and SPF regulators to act when in a position of information asymmetry.

372. We consider the current obligations on REs to act reasonably are reasonable, necessary and proportionate to balancing the desire for quality information against the achieving the purpose of the SPF.

APP 11 – Security of personal information

APP 11.1 – Protecting personal information held by APP entity

373. APP 11.1 broadly deals with the 'protection' of personal information and requires an APP entity that holds personal information to take reasonable steps to protect the information from misuse, interference or loss, as well as unauthorised access, modification or disclosure. The 'reasonable steps' an APP entity is required to take to ensure the security of personal information will depend on the circumstances, including the following:

373.1. the nature of the entity

373.2. the amount and sensitivity of the personal information held

373.3. the possible adverse consequences for individuals in the case of a breach

373.4. the practical implications of implementing the security measure, including the time and cost involved

373.5. whether any relevant security measure is itself privacy invasive.

374. The OAIC's *Guide to securing personal information, June 2018* (**Security Guide**) outlines 9 broad topics that ought to be considered when assessing how to best secure personal information held by an APP entity. The 'reasonable steps' an APP entity is required to take should, where relevant, include steps and strategies in relation to these topics. We have addressed these below except for destruction and de-identification which is dealt with under APP 11.2.

375. Databases which store information associated with the SPF will carry a high privacy risk due to the profiling required to identify high risk SPF consumers. Databases storing this information may present an attractive target for malicious third parties, who may view identified consumers as susceptible to future scam activity. Consistent with this concern, a submission from the Internet Association of Australia reported that recent data breaches saw individuals affected by a data breach experiencing increased vulnerability to scams.

376. APP entities involved in the SPF should receive guidance on the measures that would comprise reasonable steps to protect personal information, addressing the same topics as the OAIC's Security Guide (Recommendation 1). Given the high volume of personal information REs will handle, specific guidance could include:

Topic	Explanation
Governance, culture and training	• Ensure all employees are sufficiently trained in how to secure personal information and respond to data breaches. • Implement governance arrangements including risk management for information security and clear decision-making responsibilities and frameworks for managing personal information security and breaches.
Internal practices, procedures and systems	• Develop standard operating procedures for managing personal information and ASI. • Appropriately redact information from scam reports and other documents containing personal information where unnecessary for the purpose for which it is disclosed using a dedicated redaction tool (e.g. Adobe Acrobat Professional).
ICT security	• Assess whether email and network security sufficiently protects personal information and ASI, including via encryption and other measures, and if information is securely backed up.
Access security	• Restrict access to personal information to staff who need access only, and review access privileges regularly. • Keep logs of access to ASI and personal information and review audit logs regularly. • Maintaining a strong identity management and authentication framework, including through the use of passwords and passphrases.
Third party providers	• Ensure contracts with third party providers contain appropriate measures to require the contractor to handle personal information as

Topic	Explanation
	if they were the in-scope company (i.e. to take steps to protect the personal information).
Physical security	• Ensure appropriate physical security measures in relation to access to premises, devices and hard copy documents.
Data breaches	• Ensure the entity has a data breach response plan (**DBRP**) which covers responding to a data breach involving the SPF and is prepared with regard to the OAIC guide *Data breach preparation and response – a guide to managing data breaches in accordance with the Privacy Act 1988* (July 2019)
Standards	• Comply with industry standards and codes of conduct.[58] • Implement 'standards' documents for the treating of personal information and ASI under the SPF.

377. We note also that proposed s 58BS(2) (at Note 3) contemplates that approval could be given for s 58BS reports to be provided by a portal. We endorse this approach as more secure than email, which generally carries a higher risk of inadvertent disclosure and unauthorised access.

APP 11.2 – Destruction or deidentification of information

378. APP 11.2 requires APP entities to take reasonable steps to destroy or deidentify personal information that the entity no longer needs for a purpose permitted under the APPs. This obligation applies even where the entity does not physically possess the personal information, but has the right or power to deal with it.[59]

379. However, APP 11.2 does not apply where the information is contained in a Commonwealth record.[60] As a consequence, APP 11.2 will be of greatest application to REs.

380. There are no specific requirements in the SPF as to how long data such as ASI should be retained – as a result, the normal APP 11.2 obligations will apply.

381. It will be necessary to provide clear guidance to REs as to what information should and should not be retained in order to minimise potential harm in the event of a data breach. This will be particularly important where an RE has collected personal information in the investigation of potential scam activity to comply with proposed s 58BW, and identifies that a scam is not in fact occurring.

382. Destruction of personal information may occur through irretrievable destruction, or where this is not possible for electronic information, putting the information 'beyond use'.

---

58 In its submission, the Australian Finance Industry Association referred to the draft AFIA Code of Conduct which proposes to require members to take reasonable steps to protect personal information from misuse and sets guidelines for members to protect customers from scams.

59 Security Guide at p 39 citing APP Guidelines.

60 Bearing the same meaning as it does in the *Archives Act 1983* (Cth): Privacy Act s 6(1).

383. Given many REs may have concerns about destroying information in case it is later required to evidence compliance with the SPF,[61] publishing guidance on when destruction is permitted will be an important measure to prevent over-retention of unnecessary personal information (see Recommendation 1).

APP 12 – Access to personal information

384. APP 12.1 requires an APP entity that holds personal information about an individual to give the individual access to that information on request. APP 12.4 provides that access must be given within a reasonable period after the request is made.

385. APP 12 also sets out other requirements in relation to giving access, including how access is to be given and when access can be refused. There are separate grounds on which agencies and organisations may refuse to give access.

Requests for information from REs

386. Where an individual seeks access to their personal information held by an RE subject to the Privacy Act, that entity must decide whether to release the information. A consumer may request access to information held by an RE about a scam in order to take action, in order to seek compensation from an RE or to bring legal proceedings against a scammer.[62] While a consumer could make a request under APP 12, we anticipate that:

386.1. REs may disclose information about suspected scams under proposed s 58BX(1)

386.2. sector specific EDR codes made under proposed s 58BZE will address information sharing to assist a consumer to respond to scam activity.

387. APP 12.3 provides a range of circumstances in which an RE would be entitled to refuse to provide access to the personal information. These circumstances include if doing so would post a serious threat to health, life or safety, if there would be an unreasonable privacy impact on other individuals, the request is frivolous or vexatious, it would prejudice enforcement activity or denying access is required or authorised by or under an Australian law.

388. We expect there will be limited cases where REs will be able to refuse access to personal information for their own SPF consumers. None of the exceptions listed in APP 12.3 are likely to apply to this situation.

389. On the rare occasion where an RE might receive a request for access from a scammer or suspected scammer about their own personal information, we expect that REs may refuse access to personal information held in relation to the scam. The exception at APP 12.3(h) would likely apply as a scam constitutes unlawful activity that relates to the RE's functions and giving access would likely prejudice the REs ability to respond to scams in the future. This exception is also likely to apply where an RE is investigating the activity of a suspected scammer because providing

[61] A submission from the Internet Association of Australia expressed concern that REs may retain customer information for 6 years in line with the statute of limitation for civil proceedings, potentially long after the individual ceases being a customer of the entity.

[62] The submission from the Consumer Law Action Centred emphasised the importance of consumers having access to information needed to combat scams.

access to personal information in this scenario would likely prejudice the investigation. Refusing to give access to personal information in this situation would be reasonable, necessary and proportionate to achieving the purpose of the SPF and protecting Australians from scams.

390. APP 12.8 allows for APP entities to charge individuals for giving access to the personal information, but requires that the charge must not be excessive and must not apply to the making of the request.

391. While the APP Guidelines provides general guidance on APP 12, we think providing tailored guidance on responding to APP 12 requests with regards to the SPF would assist REs to comply with their obligations under APP 12 (as per Recommendation 1). This guidance should outline the reasons why an RE can refuse to provide access under APP 12.3, and the requirement to provide access within a reasonable period under APP 12.4.

Requests for information from SPF regulators

392. We expect that where an individual seeks access to their personal information held by an SPF regulator, access requests will be made and facilitated in accordance with its ordinary process and privacy policy, including applying exceptions where records are exempt under the *Freedom of Information Act 1982* (Cth).

APP 13 – Correction of personal information

393. APP 13.1 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

394. This requirement applies where:

394.1. the APP entity is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or

394.2. the individual requests the entity to correct the personal information.

395. APP 13.2 provides that if a correction is made, and the individual asks the APP entity to notify another APP entity of the correction, the first APP entity must take reasonable steps to do so.

396. APP 13.3 provides that an APP entity must advise an individual of certain matters if it refuses to correct personal information, including the reasons for the refusal and mechanisms available to complain about the refusal. APP 13.5 provides that organisations must respond to correction requests within 30 days.

397. We expect that, if individuals wish to correct personal information held about them by SPF regulators, correction requests would be made and facilitated in accordance with these agencies' ordinary processes and privacy policies.

398. Where an individual seeks to correct their personal information held by an RE subject to the Privacy Act, that entity must decide whether to correct the information. APP 13.3 provides that an APP entity must advise an individual of certain matters if it refuses to correct personal information, including the reasons for the refusal and mechanisms available to complain about the refusal.

399. Additionally, guidance should be provided to ensure that REs are aware of their obligations under APP 13 if they detect that they hold incorrect personal information, or receive a request to correct personal information. We have noted above that there may be some risk of services being withheld from individuals considered to be particularly at-risk of being victimised by scam activity. This being so, we consider that correcting personal information, such as if an RE erroneously identifies an individual as being part of a higher-risk class for proposed s 58BK purposes, will be particularly important.

400. It is possible that corrected personal information may change the outcome of a scam investigation – and that this may trigger the proposed s 58BX reporting obligations. For example, corrected personal information may constitute actionable scam intelligence or may bring the safe harbour period to an end. Guidance should alert REs to the potential overlap with their SPF obligations where correction occurs.

Annexure A – Guidance to provide to REs

Activity	APPs	Para	Matters to include in guidance
Compliance with SPF and Privacy Act	N.A	[183]	• Guidance on the intersection of the responsibilities of REs under the SPF and the Privacy Act, in particular under the Notifiable Data Breaches Scheme, with guidance on how to including meeting obligations in a non-duplicative way.
Development of governance documents and privacy policies, procedures, practices and systems	**1.2**	[213]-[214]	• Including a requirement in the SPF rules that REs prioritise protecting individual privacy when developing governance materials.
			• Specifying the kinds and volume of information REs should collect to develop governance documents so as to balance this against protecting personal privacy.
	1.3 & 1.4	[218]-[219]	• Matters an RE's privacy policy should address to reflect the handling of personal information under the SPF. • For example, the privacy policy should explain how the RE uses customer personal information to prevent, disrupt and report on, and respond to, scams, including through any use of automated decision making.
Detecting, disrupting and responding to scams	**4**	[305]	• That, if an RE collects personal information indirectly, such as through investigations of scam activity, they should update information on their website, such as a privacy policy, to ensure that relevant information is provided.
Reporting on scams	**3.2**	[267]	• Examples of template reports or the kinds of information an RE should usually obtain to facilitate reporting under proposed s 58BR.
	3.3 & 3.4	[278]	• That REs' s 58BZB reporting mechanism should clearly state an individual making a report is consenting to that report being shared with regulators.
	4	[298]	• That REs should delete any unsolicited personal information received through s 58BZB reports. • That REs be advised of potential methods for deidentifying personal information.
	4	[300]	• Clear guidance on what information REs should provide to SCF regulators in reports.
	5	[305], [310]-[312]	• That REs provide notice of the handling of personal information under the SPF at the time of collection, and the kind of matters to include in a collection notice. • When it is appropriate for an RE to provide notice of the collection, use or disclosure of a customer's personal information to prevent, disrupt or respond to a scam (e.g . a disclosure/report to Credit Reporting Bodies or temporary freezing of accounts).

Activity	APPs	Para	Matters to include in guidance
	6	[328]	• Guidance on the form of consumer notifications about scam activity, including when it is appropriate to publicly identify an actual or suspected scammer, and how an RE can provide notice without revealing methods for detecting, preventing or responding to scams.
Ensuring personal information is not used for direct marketing	**7**	[348]	• That information collected for SPF purposes should not be used for direct marketing unless an exception applies.
Ensuring personal information is of sufficient quality	**10**	[368]	• Providing examples of what might be reasonable steps to take in various scenarios with differing levels of quality of personal information. For example: - in relation to their reporting obligations, it may be appropriate for REs to cross-check scam reports they receive against other information in their possession to ensure the validity of the report. - in relation to their disruption obligations, it may be appropriate to provide guidance on the quality of information necessary to take steps such as freezing a bank account or blocking a phone number.
Protection of personal information	**11.1**	[375]	• Information relating to measures that would comprise reasonable steps to protect personal information.
Destruction of personal information	**11.2**	[381]	• Information relating to the permitted destruction of personal information.
Considering requests to access information	**12**	[391]	• That REs must give individuals access to their own personal information on request, and must do so within a reasonable time. • The grounds on which such a request may be refused, including under APP 12.3(h). • That REs can charge individuals for giving access, but that a charge must not be excessive and must not apply to the making of the request.
Correcting personal information	**13**	[399], [400]	• Information relating to REs APP 13 obligations to correct personal information. • That, if correction of personal obligation results in a change to the status of information as actionable scam intelligence, or impacts on a scam investigation, this may trigger an RE reporting obligation.

Appendix – Scope and preparation of the PIA

This PIA was conducted in accordance with the Office of the Australian Information Commissioner's (**OAIC**) Guide to undertaking PIAs in consultation with Treasury.

A full list of the documents considered by AGS in preparing this PIA is set out below.

Scope of PIA

This PIA examines the privacy impacts arising from the proposed implementation of the SPF. It describes the activities required to comply with the SPF (Part 2) and makes recommendations to minimise potential privacy risks (Part 3).

Exclusions

The scope of this PIA is limited to examining the handling of personal information as part of implementing the SPF by amending the CCA.

This PIA does not examine privacy impacts arising from the following matters:

- any obligations that the SPF general regulator or SPF sector regulators may have under the Privacy Code
- any privacy impacts arising from the implementation of delegated legislation
- SPF regulators entering into arrangements with each other
- the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)
- compliance and enforcement activities
- any conflicts with overseas laws.

Material considered in this PIA

In preparation of this PIA, we have considered the following material.

Material provided by Treasury

#	File name	Public	Provided
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

#	File name	Public	Provided
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Material identified by AGS through research

No.	Description
1.	Assistant Treasurer and Minister for Communications, Joint Media Release, *Government takes next step in fight against scams*, 30 November 2023
2.	Assistant Treasurer and Minister for Communications, Joint Media Release, *Albanese Government continues crackdown on scammers*, 21 May 2024
3.	OAIC, Australian Privacy Principle Guidelines
4.	ACCC, Targeting Scams: Report of the ACCC on scams activity (April 2023)
5.	Administrative Arrangements Orders (as at 29 July 2024)
6.	OAIC, Guide to Securing Personal Information
7.	OAIC, De-identification and the Privacy Act,
8.	OHCHR, International Covenant on Civil and Political Rights
9.	UN Human Rights Committee, General Comment No. 16
10.	Communication No. 488/1992, Toonan v. Australia
11.	OAIC, 2023 Australian Community Attitudes to Privacy Survey
12.	Scamwatch, Scam statistics
13.	ASIC, 'Anti-scam practices of banks outside the four major banks' (Report 790, August 2024) Report REP 790 Anti-scam practices of banks outside the four major banks
14.	Australian Broadcasting Corporation, While Australian banks refuse most scam victims refunds, the UK is making them mandatory
15.	UK Government, 'Fraud Strategy'
16.	*Financial Services and Markets Act 2023* (UK)
17.	Monetary Authority of Singapore and InfoComm Media Development Authority, 'Consultation Paper on Proposed Shared Responsibility Framework'
18.	*'RC' and TICA Default Tenancy Control Pty Ltd (Privacy)* [2019] AICmr 60
19.	*Johns v Australian Securities Commission* (1993) 178 CLR 408
20.	*Australian Communications and Media Authority Act 2005* (Cth)
21.	*Australian Securities and Investments Commission Act 2001* (Cth)
22.	*'WL' and Secretary to the Department of Defence* [2020] AICmr 69
23.	*AIT18 v Australian Information Commissioner* [2018] FCAFC 192

Glossary

Term	Definition
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
APPs	Australian Privacy Principles
APP entities	As defined in s 6 of the Privacy Act
ASIC	Australian Securities and Investments Commission
CCA	*Competition and Consumer Act 2010* (Cth)
DITRDCA	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
EDR	External dispute resolution
ICCPR	International Covenant on Civil and Political Rights
Privacy Act	*Privacy Act 1988* (Cth)
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not, and (b) whether the information or opinion is recorded in a material form or not.
PSP	Payment Services Providers
RE	Regulated entity
Sensitive personal information	Information defined as 'sensitive information' in s 6 of the Privacy Act
SBO	Small business operator within the meaning of s 6D of the *Privacy Act*
SPF	Scams Prevention Framework