

4 October 2024

Tom Dickson
Acting First Assistant Secretary
Market Conduct Division
The Treasury
Langton Crescent
PARKES ACT 2600
Via email: scampolicy@treasury.gov.au

Dear Mr Dickson,

RE: Consultation on Proposed Scam Prevention Framework.

The Financial Services Council (**FSC**) welcomes the opportunity to make a submission to Treasury in relation to the proposed Framework (**SPF**).

The FSC is supportive of the Government's policy intent to bring the entire scams ecosystem under a single framework that focuses on both the prevention and disruption of this criminal activity. However, the FSC believes that there is utility in considering where these obligations already exist within the wider legislative framework and leverage these obligations and frameworks, instead of creating a whole new, parallel framework that duplicates work for both industry and Government. Duplication tends to give rise to unintended consequences and confusion.

Further, there are several areas within the proposed framework that would benefit from further non-prescriptive, non-enforceable guidance, which would ensure that the SPF, outside of any separate codes, would be applied consistently between industries and entities and to provide additional clarity concerning the application and implementation of the obligations, including regulatory expectations.

For convenience, terms defined terms in the document are those as defined in *Treasury Laws Amendment Bill 2024: Scams Prevention Framework (Draft Legislation)* and the accompanying exposure draft explanatory materials to the draft explanatory memoranda (**Explanatory Materials**) unless otherwise stated.

Summary of Recommendations

1. Treasury consider how to leverage existing frameworks for scam prevention, disruption, and reporting, rather than creating an entirely separate, but only slightly different framework specific to scams.
2. Treasury provide certainty about how the Framework and a respective industry code might be enforced together.
3. Treasury should consider publishing non-prescriptive, non-enforceable guidance in relation to the Framework to ensure that, outside of the code structure, there is consistency between industry in approach.
4. Treasury insert a consideration of the utility of existing regulatory structures and frameworks into the matters that must be considered by the Minister before designating a sector under the Act.

5. That a Regulatory Impact Assessment be conducted to support the introduction of any new designated industry sector Codes.
6. There should be an explicit legislative requirement for the Minister to consult inserted into the Act before the Minister exercises their delegation power.
7. There should be an explicit legislative requirement for the Minister to consult inserted into the Act before the Minister exercises their delegation power.
8. Although there is an allowance for the creation of SPF rules to further clarify the definition of a scam, the legislation should be absolutely clear as to the delineation between fraud and scam activities.
9. Further guidance using worked examples is required to clarify and explain how an SPF consumer relationship extends to a consumer who does not have an existing legal relationship with an entity.
10. Further non-prescriptive, non-enforceable guidance should be provided in relation to the concept of actionable scam intelligence to ensure that the provisions relating to reporting of said intelligence do not result in over-reporting and undue regulatory burden.
11. It is not appropriate for organisations to publish specific or detailed information about the technology and processes being used to disrupt fraud and scam activity as this is likely to be used and exploited by bad actors. The legislation should clarify that this is not considered within the requirements of the SPF.
12. When considering an extension of the Framework to the superannuation sector, weight should be given to the impacts of KYC and EDCC at account origination on customers receiving superannuation contributions.
13. Further non-prescriptive, non-enforceable guidance is required in relation to concept of relevant resources for the purpose of preventing scams under the SPF.
14. Government should consider the implications of the need to collect large amounts of sensitive personal data and balance these with organisation's need to manage data risks.
15. Consideration should be given to how the reporting framework interacts with any existing reporting frameworks within industry and how this might be streamlined for better utility.
16. The need to report actionable scam intelligence to both regulators and consumers should be considered with a lens of utility and outcomes.
17. Further non-enforceable, non-prescriptive guidance is required as to how reasonable attempts to contact applies where an entity has no means of contacting a customer.
18. There should be an explicit notice within the legislation that there is no requirement to have an additional internal dispute resolution program for entities that are already subject to regulated IDR requirements.
19. There should be an explicit notice within the legislation that there is no requirement to have an additional internal dispute resolution program for entities that are already subject to regulated IDR requirements.

About the Financial Services Council

The FSC is a peak body which sets mandatory Standards and develops policy for more than 100 member companies in one of Australia's largest industry sectors, financial services. Our Full Members represent Australia's retail and wholesale funds management businesses, superannuation funds, and financial advice licensees.

The financial services industry is responsible for investing more than \$3 trillion on behalf of over 15.6 million Australians. The pool of funds under management is larger than Australia's

GDP and the capitalisation of the Australian Securities Exchange and is one of the largest pools of managed funds in the world.

General Feedback on Approach to Regulation

The FSC is broadly supportive of a principles-based framework approach to the regulation of scam mitigation obligations. That said, the FSC holds concerns about the utility of the proposed SPF approach in practice, in that it may lead to several extra layers of regulation, thereby increasing the regulatory burden. Consideration should be given, where appropriate, to leveraging other regulatory obligations, such as those imposed under the Anti-Money Laundering and Counter-Terrorism Financing (**AML/CTF**) regime to produce regulatory efficiencies.

Scams and fraud are predicate crimes of money laundering and accordingly, financial service providers (banks, ADIs, superannuation, remittance and virtual currency providers etc.) have obligations under Australia's AML/CTF regime. AUSTRAC is responsible for administering the regime in its combined role of regulator and Financial Intelligence Unit.

As scams are recognised globally as a serious financial or economic crime, the proposed SPF appears to duplicate the existing regulatory obligations imposed on financial institutions under the AML/CTF framework. For example, reporting entities under the AML/CTF obligation are required to:

- Establish and maintain a money laundering (ML) and terrorism financing (TF) program to identify, mitigate and manage ML/TF risks;
- Have policies, procedures, systems, and controls to mitigate and manage ML/TF risks; and
- Have an obligation to report suspicious matter reports (SMRs) to AUSTRAC where it is reasonably suspected that a crime against the Commonwealth, States or Territories has been committed. The SMR reporting obligation is an all-crimes approach, and this clearly encompasses scams including investment scams, romance scams, product and services scams, identity theft, threats and extortions and job and employment scams.

The AML/CTF regime is not only complex, but also resource-intensive because it imposes an extensive range of compliance and reporting obligations on regulated entities, involving detailed policies, procedures, systems and controls. In order to enforce compliance, AUSTRAC has available a comprehensive and extensive toolkit to enforce compliance, ranging from administrative actions through to civil penalties, and in some instances, criminal penalties.

AUSTRAC's partner agencies comprise law enforcement, national security, revenue protection, anti-corruption agencies as well as regulatory agencies such as the ACCC, APRA and ASIC. These agencies can access the AUSTRAC database either directly online or AUSTRAC can proactively disseminate this information.

There is currently amending legislation before the Australian Parliament to reform the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), which will require regulated entities to invest in uplifting their current frameworks and systems. The reforms include among other things, the loosening of restrictions on the sharing of SMR information (also known as tipping off) to enable effective and efficient public-private and private-private information sharing arrangements to combat serious financial crime.

The FSC submits that for entities already subject to AML/CTF compliance, creating an almost identical regime that focuses solely on scam activities is an inefficient and ineffective use of resources for industry and government. Regulated sectors under the AML/CTF regime already have mandatory reporting obligations in relation to scam activity. Having to submit dedicated and tailored reporting in response to scam activity will create inefficiencies in the system, and it is unclear how this will ultimately benefit consumers. For example, it will be necessary to clarify the roles and responsibilities of AUSTRAC as the national financial intelligence unit, its law enforcement partners responsible for investigating serious financial crime, and that of the ACCC (National Anti-Scam Centre).

Duplicate or overlapping regulations and legislation may give rise to unintended consequences and confusion since there is, at times, drafting uncertainty in the duplicating legislation or regulatory guidance. Government should consider leveraging existing regimes where possible, and filling gaps where necessary.

RECOMMENDATION 1

Treasury consider how to leverage existing frameworks for scam prevention, disruption, and reporting, rather than creating an entirely separate, but only slightly different framework specific to scams.

Notwithstanding the above, the FSC submits that in order for the best possible consumer outcomes to be achieved, there needs to be consistency of approach across industry sectors as to how the framework is to be applied.

Further, because an industry code would be enforced by the respective regulator, but the SPF itself is enforced by the ACCC, there may be inconsistencies in these approaches, creating further uncertainty for industry.

While the FSC is supportive of the approach, industry would benefit from some certainty about how the enforcement responsibility would likely be shared between the two respective regulators and how consistency of approach would be ensured.

RECOMMENDATION 2

Treasury provide certainty about how the Framework and a respective industry code might be enforced together.

Additionally, regulated entities operating under individual sector codes will require written guidance to assist in understanding and implementing their obligations, and this should also include regulatory expectations, the use of worked examples to explain the practical application of obligations, and the intended approach to regulation and enforcement, noting that the framework involves multiple regulators. This guidance should not be legally enforceable and should be subject to stakeholder consultation.

Provision of this guidance would have the added benefit of ensuring that subsequent codes that fall under the Framework are consistent in their application and implementation, in so far as possible, across industry sectors.

RECOMMENDATION 3

Treasury should consider publishing non-prescriptive, non-enforceable guidance in relation to the Framework to ensure that, outside of the code structure, there is consistency between industry in approach.

The FSC is supportive of the ability for the Minister to later designate sectors to which the SPF will apply, resulting in the provision of a separate mandatory code. Within the Exposure Draft there is a list of matters the Minister must consider. While the FSC is supportive of this list, it is recommended that it be extended to include consideration of any existing, complementary regulatory frameworks appropriate to the designated sector.

Within the superannuation sector, there already exists significant prudential architecture in relation to the mitigation of scam activities, and this is further complemented by AML/CTF compliance and reporting obligations and other scam/fraud compliance mechanisms. While there may be merit to a code that covers the superannuation sector, we are concerned that without proper consideration of existing obligations, this would constitute an additional layer of regulatory burden, and it is important that consideration be given to leveraging existing obligations as part of any deliberations to alleviate the impacts.

By including the consideration, applicability and appropriateness of existing regulatory frameworks before designation, this ensures that certain industry sectors are not committing resources required that duplicate existing obligations in scam and fraud prevention. The ability to consider and leverage opportunities for regulatory efficiencies is consistent with a prudent and efficient regulation agenda.

RECOMMENDATION 4

Treasury insert a consideration of the utility of existing regulatory structures and frameworks into the matters that must be considered by the Minister before designating a sector under the Act.

Additionally, the FSC considers that in line with better regulation practices, it would be prudent to undertake a Regulatory Impact Assessment as part of the designation a new industry sector code.

RECOMMENDATION 5

That a Regulatory Impact Assessment be conducted to support the introduction of any new designated industry sector Codes.

The FSC submits that before the Minister exercises their designation power, there should be a legislative requirement to consult with the affected industry sector. This would give certainty to industry about the pipeline of potential regulatory change.

RECOMMENDATION 6

There should be an explicit legislative requirement for the Minister to consult inserted into the Act before the Minister exercises their delegation power.

Industry would benefit significantly from a coordinated cross-government scams, fraud, and cybersecurity strategy. The proposed Framework does not appear to consider the likely impacts of current work happening across government in relation to not just scams, but also other forms of cyber and economic crime, including cybersecurity.

A coordinated approach would bring together significant pieces of work such as these proposed codes, the work of the National Anti-Scams Centre (NASCC), and the National Cyber Security Strategy as well as more targeted pieces of work such as the implementation of the Digital ID Framework, proposed revisions and enhancements to Anti-Money Laundering and Counter Terrorism Financing (**AML/CTF**) and privacy legislation, and individual regulator actions. This would provide much needed certainty and a clear set of goals.

There is some concern that some of the work happening across government is incongruent and may lead to conflicting expectations placed on organisations, thereby increasing the regulatory burden. For example, there is a strong push for organisations to collect less sensitive data to protect against cyber-attacks, but that sensitive data is exactly what may be needed for intelligence purposes that is used to combat scams and fraud.

A consistent and coordinated strategy would benefit both Government, regulators, industry, and consumers to understand the clear vision to protect Australians from the harms of economic and cybercrime.

RECOMMENDATION 7

Government considers creating a whole-of-government scams, fraud, and cybersecurity strategy that clearly outlines goals for protecting Australians from the harms caused by economic and cyber-crime.

Meaning of a Scam

The definition of scam within the exposure draft legislation, broadly defined to involve deception and an action that would cause loss, is, as noted within the draft Explanatory Memorandum, designed to be wide. However, the definition may be too broad and may include conduct that is not typically thought of as scam behaviour. The FSC does not support a broad legislative definition of a scam, notwithstanding the ability for rules and regulations to be subsequently made in relation to this definition. The FSC believes the overarching legislation should be clear about what is a scam.

The exposure draft legislation defines a scam as:

- a. deceptively represents something to be (or to be related to) the regulated service; or
- b. deceptively impersonates a regulated entity in connection with the regulated service;
- c. is an attempt to deceive the SPF Consumer into facilitating an action using the regulated service; or
- d. is an attempt to deceive the SPF Consumer that is made using the regulated service.

This definition may capture cases of fraud where a person utilises their power of attorney or equivalent to the benefit of the fraudulent party. In these circumstances this would be dealt with under the existing fraud framework.

From the list of examples within the exposure draft legislation, it would appear that cases of fraud that are the result of another scam (for example, a phishing scam) appear to be

excluded. If this is the case, then the example cited above should also be clearly excluded as they are dealt with elsewhere.

It is noted that there is an allowance for the SPF Rules to prescribe carve outs for what is not a scam, and the FSC is supportive of the list presented in the draft Explanatory Memorandum as a starting position for what should not be considered a scam.

That said, the FSC submits that scam specific legislation should be absolutely clear in its scope so that the delineation between fraud and scams is clear. This may additionally require supporting guidance and incorporate worked examples to provide the additional clarity.

RECOMMENDATION 8

Although there is an allowance for the creation of SPF rules to further clarify the definition of a scam, the legislation should be absolutely clear as to the delineation between fraud and scam activities.

Scam Protection Framework Consumer

The FSC is broadly supportive of the definition of an SPF Consumer. While there is utility in protecting consumers by ensuring a relationship extends between a person who does not have a legal relationship with a regulated entity, the FSC submits there should be clear guidelines/guidance concerning the expectations of those entities.

Naturally, an entity with a legal relationship with a consumer owes that consumer a certain level of protection and under the new scams framework, it is reasonable to expect entire industries to share a level of responsibility for the whole ecosystem. However, it is unreasonable that an entity with no prior legal relationship or link, and therefore no prior knowledge of a specific consumer, would have the exact same level of oversight and responsibility as an entity that did have that had a formal relationship.

Further guidance using worked examples will be required to clarify how these relationships will work in practice.

RECOMMENDATION 9

Further guidance using worked examples is required to clarify and explain how an SPF consumer relationship extends to a consumer who does not have an existing legal relationship with an entity.

Actionable Scam Intelligence

There are several requirements within the Exposure Draft Legislation related to actionable scam intelligence, including a requirement to act on and report said intelligence. Actionable scam intelligence has a broad definition and is prescribed with a reasonableness test for assessing whether action is appropriate.

While acknowledging the objective behind this intended policy outcome, the FSC submits that a requirement to report actionable scam intelligence to both customers and regulators in all instances will create a significant regulatory burden, given the broad definition of the term, and particularly where there is an existing obligation to report by those entities subject to AML/CTF obligations.

While it may be appropriate at the legislative level to have a broad definition of actionable scam intelligence, the FSC believes further non-prescriptive guidance is warranted to ensure that organisations are applying the standard consistently and to ensure that the right level of actionable threat is being reported, rather than every single piece of potential intel that an organisation may have.

The FSC will make further comment on this in the relevant sections below.

RECOMMENDATION 10

Further non-prescriptive, non-enforceable guidance should be provided in relation to the concept of actionable scam intelligence to ensure that the provisions relating to reporting of said intelligence do not result in over-reporting and undue regulatory burden.

Scams Prevention Framework Principles

The FSC is broadly supportive of the principles outlined in the Exposure Draft legislation however, as noted above, there already exists a framework for the prevention, disruption and reporting of scam activity in Australia through the AML/CTF framework.

Notwithstanding the FSC's recommendation that this framework be leveraged so as not to duplicate effort, the FSC makes comment in relation to some more specific matters below.

Further, and as previously noted, industry would greatly benefit from further, non-prescriptive, non-enforceable guidance to help provide consistent approaches between entities.

Governance

Under the Governance part of the Framework, entities are required to make public the steps taken to protect consumers from scams. The Exposure Draft Legislation specifically mentions publishing the 'measures' it has in place to protect consumers but goes on to say that an entity does not need to publish all policies, procedures, and metrics. In the Explanatory Memorandum, it is noted that this might include "such information about technology to block suspicious transactions..."

It would not be appropriate for an entity to have to publish *specific* measures it takes to protect consumers from scams, including any fraud detection activities and processes undertaken therein. This would allow scammers, which primarily involve sophisticated serious and organised crime groups domiciled in foreign countries, to undermine and exploit the work industry does in relation to fraud and scam mitigation by essentially pointing out the defences.

The definition in the legislation is unnecessarily broad and should instead focus on what is appropriate to be published in a consumer facing forum, noting that the designated industry Code will be accessible and outline the responsibilities of each regulated entity. Other measures outlined in the Explanatory Memorandum including how customers can report scams and how they can make complaints are appropriate to be published and the FSC is supportive of limiting the definition to these.

RECOMMENDATION 11

It is not appropriate for organisations to publish specific or detailed information about the technology and processes being used to disrupt fraud and scam activity as this is likely to be used and exploited by bad actors. The legislation should clarify that this is not considered within the requirements of the SPF.

Prevent

Specific measures relating to the use of identity checking in the superannuation context.

The FSC notes that the specific prevention tactics that individual industries must implement will be left largely to industry codes, however, the Explanatory Memorandum makes note that this may include the need for additional identity verification requirements for new accounts. While the FSC understands that this Framework and any subsequent codes are not yet to extend to the superannuation industry, the FSC would like to take this opportunity to bring the Treasury's attention an issue pertaining to this matter.

The FSC is not supportive of placing identity checking, also known as Know Your Customer (**KYC**) or applicable customer identification procedure (**ACIP**) and/or Enhanced Customer Due Diligence (**ECDD**) obligations at the account open phase of the customer journey, noting that these obligations under the AML/CTF Act exempt superannuation funds on joining the fund or conducting roll-overs. The obligation for KYC applies where a member of superannuation fund seeks access to funds (i.e. payment), such as a hardship claim or converting to a pension on retirement.

There are significant legislative and practical barriers to making this a requirement of the onboarding process including that the KYC requirement may disrupt the allocation of superannuation contributions, be difficult to implement on accounts not opened directly by the individual, and, if not extended to employer opened accounts, may create a perverse outcome that discourages choice of fund.

The AML/CTF regime is an important part of the suite of measures protecting Australia from financial crime, and KYC also has a role to play in protecting customers from the risk of fraud. It should be noted that funds already have obligations under the AML/CTF framework to proactively monitor client accounts to identify, mitigate, and manage changes in the levels of financial crime risk arising from unusual account related activities or client behaviours.

This includes scams and fraud as predicate offences under the AML/CTF laws. If a fund has concerns regarding the activity or behaviour concerning a client account, it is a trigger for conducting ongoing and/or enhanced customer due diligence, which includes among other things, KYC and ECDD requirements, and depending on the circumstances, submitting a suspicious matter report to AUSTRAC.

Further, KYC can be performed when a customer seeks to transact on their account, either to withdraw a lump sum on retirement, convert to a pension, submit a hardship claim, or rollover into another fund or SMSF, in addition to any additional security checks a superannuation fund may choose to perform. This is an appropriate time to KYC a customer because, if it is indeed the customer requesting the transaction, they will be actively engaged in the process and can provide the appropriate identification in a timely manner.

The AML/CTF Amendment Bill currently before the Australian Parliament does not propose to change the current legislative exemption to conduct KYC processes for superannuation at the point of joining a fund and reinforces the risk-based approach.

One of the key issues with placing the requirement to identify a customer at account open is that it could disrupt the allocation of superannuation contributions into the account because, in theory, if the account has not had the appropriate identity checks, a fund cannot allocate the contributions to it. While this has the potential to stop the creation of some fake accounts for criminal purposes, it will also have the unintended, and arguably more significant impact of potentially stopping a person's and their employer's contributions from flowing into their account, impacting their earnings and balances at retirement.

Unlike banks, which can simply reject funds if the customer has not provided KYC for the account, superannuation funds have a legislated obligation to allocate funds within specific timeframes. Typically, where an employer sends a person's contributions to a fund and they cannot be allocated (because of a data entry error or otherwise), the funds are sent back to wherever they came from.

Given the Government is looking to move to a payday superannuation model, which will already significantly increase the number of transactions across the Superannuation Transaction Network¹, KYC on account open would likely delay the payment of superannuation transactions for a not-insignificant number of customers. Further, and as noted in the FSC's response to Treasury's payday super consultation, this will likely increase the error rate of contributions that cannot be allocated by a superannuation fund. In that response, the FSC noted that the compounding of the errors at the superannuation fund end could cause significant administrative burden, and delayed payments.

The FSC also submits that this type of regulation may create a situation where it is easier for an employer to open a superannuation account on behalf of an employee if those identity checking requirements are not applied equally to an employer opened, versus directly opened account. Although there are some obligations on employers to identify an employee upon commencement, this does not necessarily amount to KYC or ECDD on behalf of an employee if they were to open an account in a default fund for them. While there are often good reasons for an employee to choose to go with an employer sponsored fund, it should not be the case that one process is easier than the other. Choice remains an integral component of the superannuation system and placing an impediment that actively discourages choice strikes at the heart of that tenet and could be anti-competitive.

Under the existing AML/CTF framework, organisations are required to ensure that they are monitoring customer behaviour for suspicious transactions. FSC members currently do this in myriad ways and are actively investing more and more into innovative systems that can help them manage their economic crime risk.

Given the struggles with implementing KYC at account open, the FSC submits that superannuation funds are better off managing their risk in a way that works for their operational model, in line with their duty to act in the best financial interests of customers.

RECOMMENDATION 12

When considering an extension of the Framework to the superannuation sector, weight should be given to the impacts of KYC and EDCC at account origination on customers receiving superannuation contributions.

¹ Commonly referred to as 'STN' is the is a network developed to assist employers and superannuation funds meet their obligations under the mandatory [Data and Payments Standards](#).

Relevant Resources

The Exposure Draft Legislation also requires that an entity make relevant resources accessible to consumers to identify scams and minimise the risk of harm. Further non-prescriptive, non-enforceable guidance about the form and function of these relevant resources is required to ensure a consistent approach across industries. For example, relevant guidance would note if it sufficient for an organisation to have a section on the website with the relevant information or whether an organisation needs to contact customers directly.

RECOMMENDATION 13

Further non-prescriptive, non-enforceable guidance is required in relation to concept of relevant resources for the purpose of preventing scams under the SPF.

Collection of Personal Data

Although not expressly captured by the SPF consultation, the FSC submits that the collection of personal data presents a significant risk of data breaches. The data stolen during a data breach can be used to later commit fraud. Government should further consider ways to protect both consumers and organisations from these harms including:

1. How best to legislate the collection of primary identity data;
2. The security requirements and oversight for those that do collect
3. Educating the public about best practice protective behaviours through advertising and trusted resources to encourage the community to refrain from oversharing data.

Similarly, in legislating the SPF, Government should consider how increased identity checking, and verification requirements impact the cybersecurity landscape, and entities need to protect pools of personal data.

RECOMMENDATION 14

Government should consider the implications of the need to collect large amounts of sensitive personal data and balance these with organisation's need to manage data risks.

Report

The FSC is supportive of a framework that encourages better reporting of scam activity, particularly between entities. For this reason, the FSC is supportive of the consideration given to providing certainty to entities about their obligations under other legislative frameworks in relation to reporting and sharing private information.

That said, it is important to recognise that many organisations, particularly those within the financial services sector have existing reporting frameworks, for example, the AML/CTF Act and the suspicious matter reporting regime. Any reporting requirements should be consistent with these, and consideration given to the provision of a one-stop shop for the reporting of scam and fraud activity which would allow all relevant Government parties to receive scam and fraud reporting from an entity in a simplified way.

It is noted, for example, that AUSTRAC operates as Australia's financial intelligence unit and is responsible for disseminating actionable intelligence to its domestic partners in law

enforcement, national security, criminal intelligence, revenue protection, and regulation, including the ACCC, ASIC and APRA, These agencies can access this intelligence either directly online or it is proactively disseminated by AUSTRAC. Such an outcome would result in regulatory efficiencies by not duplicating reporting obligations.

It may be possible for Treasury to work with AUSTRAC and industry to develop a tailored SMR report specifically for scams to accommodate and align with the ACCC's requirements.

RECOMMENDATION 15

Consideration should be given to how the reporting framework interacts with any existing reporting frameworks within industry and how this might be streamlined for better utility.

As noted above, the definition of actionable scam intelligence is broad and non-specific. The requirements in the reporting part of the SPF will require funds to report a significant amount of information under this standard.

Consideration should be given to the actual expectation of reporting to both customers and enforcement agencies to ensure that there is utility in what is being reported and genuinely actionable and urgent reporting does not get lost in the noise of a wide range of reports.

RECOMMENDATION 16

The need to report actionable scam intelligence to both regulators and consumers should be considered with a lens of utility and outcomes.

Disrupt

Under the disrupt portion of the SPF, there is a positive duty to take steps within a reasonable time period to notify a SPF Consumer that they may be at risk of scam activity. While the FSC notes the reasonable steps requirement, there may be instances where an entity does not have the contact details of a person.

In the superannuation context there are two examples:

- a. The person has opened their superannuation account many years ago and has not kept their contact details up to date;
- b. The account is a staging account, opened by a person with stolen credentials to aide in moving money around the system as a result of a scam or fraud activity.

Guidance is required about the meaning of reasonable in this context to ensure that funds that do not have access to contact information are given certainty as to the extent of its obligations.

RECOMMENDATION 17

Further non-enforceable, non-prescriptive guidance is required as to how reasonable attempts to contact applies where an entity has no means of contacting a customer.

Respond

The respond portion of the Framework requires that organisations have an Internal Dispute Mechanism in place. Superannuation funds and other financial services organisations already have a requirement to have such a mechanism in place and the FSC submits that

any legislative framework should acknowledge that existing required frameworks are sufficient for the purposes of the legislation.

This is to ensure that there is no double up of requirements creating additional regulatory burdens.

RECOMMENDATION 18

There should be an explicit notice within the legislation that there is no requirement to have an additional internal dispute resolution program for entities that are already subject to regulated IDR requirements.

The FSC understands that in applying the intention to apportion liability across the whole of the scam ecosystem, all SPF regulated entities would need to join the Australian Financial Complaints Authority (AFCA). The FSC has previously supported a no-wrong-doors approach to this type of complaint resolution and supports the expansion of AFCA's powers to determine cases across the whole ecosystem.

That said, further guidance is needed to understand how the apportionment of liability is expected to be carried out by AFCA. It is important that all entities along the lifecycle of a scam do their part to ensure that a scam is not successful. If this is not outlined clearly through legislation, it will leave the matter open to interpretation and may lead to inconsistent decision making. As superannuation funds and banks are the custodians of the money, which is subject to the scam, there is concern that these entities may do everything within their obligations and still receive more apportionment of liability than necessary.

RECOMMENDATION 19

Clear expectations should be set for the SPF External Dispute Mechanism to ensure there is clarity around how each individual entities obligations and liabilities will be apportioned during a complaint.

If you have any questions about the content of this submission, please do not hesitate to get in contact.

Yours sincerely,

Kirsten Samuels
Policy Director, Superannuation and Innovation