



FINANCIAL
CRIMES
EXCHANGE

Scams Taskforce
Treasury
1 Langton Crescent
Parks ACT 2600

Dear Treasury

Scams Prevention Framework – exposure draft legislation

The Australian Financial Crimes Exchange (**AFCX**) welcomes the opportunity to make a submission to the Scams Prevention Framework – exposure draft legislation (**Bill**).

AFCX supports a legislative regime that applies to relevant sectors and entities in the scam ‘ecosystem’, and the introduction of a single external dispute resolution scheme. AFCX also supports the sharing of useful and actionable information.

Reducing the time between identifying and disrupting the scam will help to reduce the number of Australians that may be exposed to, and therefore suffer harm from, a scam.

Key recommendations

AFCX’s submission focuses on further enhancing the effectiveness of information sharing arrangements in the Bill. Our key recommendations are:

- Amend the definition of ‘actionable scam intelligence’ to focus on information that can be used to identify specific scam activity or actors.
- Give the general regulator powers to specify the data that should be shared and the types of intelligence sharing arrangements that can be used, to provide flexibility while ensuring the general regulator can perform its broader information sharing function.
- Ensure legislation allows the use of automation to share actionable intelligence, to enhance efficiency.

Additional comments are set out in the detailed submission. If you have any questions about this submission, please contact Rhonda Luo at rhonda.luo@afcxc.com.au.

About the Australian Financial Crimes Exchange

AFCX helps industry and government to combat fraud, scams and other financial crime. AFCX provides a secure and trusted platform where participating organisations share and gain critical data and insights from each other. This enhances the identification, investigation, and prevention of financial crime, and protects the organisations and their customers.

AFCX is supporting the work of the National Anti-Scam Centre, including by using the Intel Loop to share scam intelligence across sectors to facilitate takedown, divert or disrupt scam communications and prevent further harm.



Detailed submission

Actionable scam intelligence

The Bill would establish a regime that requires regulated entities to share, and act on, actionable scam intelligence. The Bill would also require regulated entities to report on actions taken in response to each actionable scam intelligence.

AFCX strongly supports intelligence sharing, within and between regulated sectors.

AFCX provides suggestions to enhance the effectiveness of the regime relating to sharing actionable scam intelligence. In particular, ensuring useful and accurate intelligence is shared with a minimal of 'noise' (errors, incidents that are not scams, or information that is not 'actionable'), and that regulated entities focus on taking action to identify and disrupt scams when they receive intelligence.

Defining actionable scam intelligence

AFCX suggests that the definition of 'actionable scam intelligence' in section 58AI should refer to information that regulated entities can use to identify a specific scam transaction or activity, or a specific account, profile or person conducting the activity.

Rationale:

AFCX considers this definition could be more targeted. Actionable scam intelligence:

- need to be accurate and reliable;
 - The proposed definition may capture information about transactions that may not be a scam, reducing the reliability of information shared under this regime. This can weaken the impact of intelligence sharing, if entities take longer to investigate each report or miss a scam among the 'noise'.
- should be able to pinpoint a particular scam activity;
 - The proposed definition could capture a description of a trend or how the scam may appear to a consumer, which can differ from the information that can be used to pinpoint a particular transaction or account.
- should be defined by reference to what can be done with the information rather than the source of information.
 - Information from some sources can be a mix of actionable intelligence and other, more general, information that is not actionable.

General regulator to prescribe certain matters

AFCX suggests the general regulator could have the powers to prescribe information that constitute actionable scam intelligence for each sector, as well as principles-based expectations for what kind of third-party intel-sharing arrangements can be used.



Rationale:

A prescription power would help the general regulator to ensure the intelligence-sharing regime in the Bill is adapted to existing or future intel-sharing arrangements, including third-party arrangements, and the information shared is fit for purpose for the regulated sectors:

- Actionable intelligence for a social media platform may be the link to the relevant advertisement or page. The same information would not help to identify scam activity in relation to a telecommunications or banking services, or a messaging service operated by a digital platform. Future sectors in the Scams Prevention Framework regime may require specific information, such as about cryptocurrency wallets.
- AFCX understands the policy intention is to allow some third party intelligence-sharing arrangements to be used to meet this regulatory obligation. This is not currently provided under the Bill. It may be useful for the general regulator to have the ability to specify what types of third party arrangements can be used, and any principles based outcomes or expectations (such as the timeliness of intel-sharing)

Automation and use of technology

AFCX suggests that legislation could be drafted in a way that enables the use of automation to send and receive actionable scam intelligence between regulated entities, with no or a minimal of manual handling by the general regulator. This can be in addition to the general regulator's information sharing function under proposed subsection 58BU(1).

Rationale:

Under the proposed intelligence-sharing regime, regulated entities may share and/or receive a significant volume of information. Efficiency is of the essence when we seek to reduce the time between identifying a scam and disrupting the scam at scale. If there is delay in taking action, those scams will remain 'live' for longer, with more Australians potentially being exposed to the scams and potentially losing money to the scams.

Proposed s58BU(1) provides the general regulator may share information with another person if the general regulator reasonably believes that doing so will assist in achieving the object of Part IVF. This may require the general regulator to review a piece of information and make a decision that the information should be shared.

This outcome can create a resource-intensive requirement for the general regulator to share information in close to real time. When there is a spike in cases, this step can delay intelligence sharing at a critical time.

Supporting automation allows regulated entities to process a larger volume of information and/or realise operational efficiencies, in order to act quickly and effectively. An example is sending and receiving intelligence via an API.



Technology can help to improve the accuracy of intelligence by standardising how information is reported and shared. This may be particularly relevant when sharing intelligence across multiple industries that may be unfamiliar with each others' requirements and processes.

Acting on intelligence

AFCX supports the Bill's intention to ensure regulated entities investigate and act on intelligence provided by other organisations. AFCX notes that entities may take one action that applies to a number of reports, before or after the intelligence is received, and suggest section 58BW could accommodate this outcome.

Only using intelligence for intended purpose

AFCX asks the government to consider whether it may be appropriate to require entities to only use intelligence for the purposes of investigating, identifying, disrupting, preventing or responding to scams, and only to disclose the information to another party for the same purpose.

Additional comments

AFCX also provides comments on other aspects of the Bill to the extent they relate to information sharing and reporting.

Differences between intelligence, consumer warnings and other reporting

Consumer warnings: AFCX notes a number of stakeholders have proposed amendments to the Bill that would reduce the number of notifications that consumers may receive, and supports this outcome as it can help to reduce notice fatigue for consumers that may paradoxically reduce the effectiveness of consumer warnings.

Regulator reporting: AFCX considers it can be important to clearly distinguish between time-critical intelligence sharing and other regulatory reporting. AFCX also notes some information that may be prescribed for a s58BR or s58BX report may not be available at the time the report is required to be submitted.

- Full information about the form of loss or harm resulting from a scam may not be known to the regulated entity when it is required to provide a report under s58BR(1). In cases where there is a prospect of funds recovery, the actual loss in some cases may not be known when the entity is required to provide a report under s58BX(2) because the entity has determined whether or not a report is a scam in accordance with s58BZ(2)(d).
- Depending on the regulated sector and how scam activity is identified on an entity's service or platform, the entity may not have all demographic information when the entity is required to provide a report under s58BR(1). This could be the case for a telco.
- AFCX questions whether all regulated entities may have the information required in accordance with s58BX(5)(b), and the policy intent of reporting in accordance with s58BX(5)(c).



AFCX suggests the general regulator could determine the specifics of regulatory reporting and the frequency of reporting that is required to carry out relevant functions and duties, while balancing considerations like data minimisation. AFCX notes periodic reporting could be drawn from existing data, subject to the appropriate level of due diligence.

Timing for bringing other sectors into the Scams Prevention Framework regime

AFCX asks the government to consider an expedited timetable for bringing additional sectors into the Scams Prevention Framework, including payments and cryptocurrency. Scammers use different means of transferring money or value to conduct illicit activities, and pivot quickly in response to controls applied by banks and other institutions. As such, enhancing controls and protections in the banking sector could result in illicit transfers moving to non-bank channels.

Law enforcement information-sharing

AFCX has also consulted with stakeholders including International Justice Mission (**IJM**) about data sharing that can facilitate domestic and cross-border law enforcement outcomes. As the government would be aware, the AFCX has a history of facilitating collaboration between the banking industry and law enforcement.

While prosecution cannot stop scams from happening, they can have a deterrent effect that helps to make Australia a less attractive place for these criminals to operate. They can also result in funds recovery for Australian scam victims where perpetrators are successfully identified, as per a recent outcome reported by the Australian Federal Police's JPC3 as a result of their collaboration with international law enforcement and a cryptocurrency provider following a consumer's report to their bank and local police .

In relation to scams, it is crucial to tackle the overseas compounds where migrant workers are being trafficked and forced to scam consumers and businesses in other countries, often using enabler platforms like social media and messaging services. For these cases, collaboration between Australian and overseas law enforcement is key.

Law enforcement operates across multiple levels in Australia and overseas, with potentially disparate sources of intelligence. In IJM's experience, creating a 'clearing house' to centralise intelligence from the private sector and make it available to law enforcement can help focus resources and obtain enforcement outcomes. Relevant intelligence for scams includes cryptocurrency and IP addresses associated with these activities – noting that industry and law enforcement have the capabilities to trace these transfers.

For example, the US-based National Center for Missing and Exploited Children (**NCMEC**) operates a CyberTipline as a designated reporting mechanism for members of the public and electronic service providers to report instances of suspected child sexual exploitation. NCMEC then makes CyberTipline reports using reported data and their additional analysis available to local and international law enforcement for prioritisation and investigation.

AFCX, in conjunction with IJM, asks the government to consider establishing a similar information sharing arrangement in Australia to facilitate improved law enforcement



FINANCIAL
CRIMES
EXCHANGE

investigation and collaboration to tackle the ‘source’ of scams. AFCX notes the general regulator has the power to share intelligence with other organisations [including law enforcement – double check]; this can bridge between scams intelligence and a proposed clearing house which could be managed by law enforcement or a regulator (e.g. JPC3 or the National Anti-Scam Centre).

AFCX also notes existing data sharing technologies can be adapted, with appropriate legal protections and governance, to facilitate such an initiative.



FINANCIAL
CRIMES
EXCHANGE