

Introduction

This document is provided in response to the exposure draft of the 'Scams Prevention Framework' and call for industry comment.

The Financial Sector – Information Sharing and Analysis Centre (FS-ISAC) is grateful for the opportunity to represent our members with operations in Australia and commend Government for inviting industry to participate in this consultation process.

Our submission will primarily focus on the question of building a '*...coordinated intelligence sharing ecosystem by mandating timely reporting and information sharing across industry and government.*' This is closely aligned with FS-ISAC's role and function.

Who is FS-ISAC?

General overview

FS-ISAC is the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions, and in turn their customers, it leverages its intelligence platform, resiliency resources and a trusted peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

The Global Intelligence Office (GIO) is staffed by a mix of intelligence, cyber and technical analysts. The team is geographically divided into three regions: Asia-Pacific (APAC), Europe and Middle East (EMEA) and the Americas (AMER). GIO develops its own intelligence outputs, in addition to the publication of member submissions to the financial sector.

FS-ISAC is headquartered in the United States, with regional offices in Singapore and London. As a not-for-profit and member-driven organisation, we represent approximately 5,000 financial sector members in 75 countries.

In addition to its membership, FS-ISAC has established formal sharing arrangements with a range of law enforcement bodies (e.g. Interpol), CERT organisations (e.g. TB-CERT in Thailand) and ISAC bodies (e.g. F-ISAC in Japan).

Intelligence sharing as core business

The core business of FS-ISAC is to facilitate the sharing of intelligence that is relevant to the security of the global financial sector. This includes intelligence on cyber threats, also fraud and scam activities. The secure platforms and mechanisms we use for intelligence sharing are detailed in *'Appendix A: Intelligence sharing as core business.'*

Australian footprint

In February 2022, FS-ISAC was incorporated as a legal entity in Australia, and immediately established a Deed of Confidentiality with the Australian Cyber Security Centre (ACSC). Board representatives consider further expansion in Australia desirable given its Five Eyes status, its role in global financial operations and its broadly its stable economic and political environment.

FS-ISAC have three full time, ongoing staff located in Australia:

- ▶ Lisa Jane Young (APAC Intelligence Officer / Melbourne)
- ▶ Rachael Weston (APAC Intelligence Analyst / Sydney), and
- ▶ Lachlan Pope (Regional Director, Australia / Sunshine Coast).

Approach and consultation

This submission briefly summarises the opportunities, risks, concerns and questions that have been highlighted by FS-ISAC members.

Input was gathered via a consultation meeting on 20 September 2024. This was attended by 56 FS-ISAC members with operations in Australia. Participants are associated with a range of sectors including (but not limited to) banking, insurance, investment firms and payment processors.

Proposed reporting obligations

Preferred reporting mechanism

FS-ISAC members noted the range of mandatory and elective avenues for reporting scams and financial crime activity in Australia. Examples include ScamWatch, AUSTRAC, ACC, APRA and ASIC. The Australian Financial Crimes Exchange (AFCX) also operates as an independent, non-profit reporting channel for financial crimes.

Our members seek clarification as to which (if any) of these will continue following implementation of the proposed legislation. Breach notifications may also potentially overlap – or conflict with – scam and other reporting obligations.

The financial sector has a strong preference for a single reporting portal for Government to minimise potential errors and impacts on available resourcing. A single portal for fraud, scams and cyber threat activity is preferable, given the nature of functional overlaps (see also: Legislative and global complexity).

If a single portal cannot be established, Government may consider providing technical support to organisations that are within scope of the new reporting obligations to help integrate the new requirements into existing architectures.

FS-ISAC also facilitates the sharing of scam intelligence for both Australian and global financial sector operations. While scam operations are global by nature, the Scam Prevention Framework is silent on the question of global activity (such as government co-operation or the provision of trend data and scam intelligence).

Several members have asked whether FS-ISAC can facilitate the reporting of scams to Government. While this is not viable, we are open to providing scam trend intelligence based on member reporting to the Australian Government. This would necessarily be at the TLP Green level.

While seeking a simple, centralised reporting process, FS-ISAC members note the potential for this to create a concentration risk, given the growing incidence of cyber-attacks and human errors resulting in data leakage.

Extent of reporting obligations

A key question posed by FS-ISAC members is the *extent* of the proposed reporting obligations for scam activity. While the initial scope is confined to banks (for the financial sector), it is not clear whether the requirements include banking clients and/or third parties.

Further clarification is also needed on the specific *types of information* that must be reported under the new legislation, particularly in the context of privacy obligations.

Non-bank members seek early warning if the scope for scam reporting is to expand (including advice on the specific portions of the final sector impacted and expected timeframes for inclusion).

Increased obligations to report scams may have a disproportionately large impact on resourcing for non-bank elements of the financial sector. Many smaller financial sector organisations do not yet incorporate a dedicated fraud function.

Intelligence and industry support

FS-ISAC notes that the 'Prevent > Detect > Report > Disrupt > Respond' elements of the Scam Prevention framework are presented as a unidirectional sequence of events. However, a reconceptualization of this as a recurring loop is likely to offer additional benefits. The analysis of scam reports to provide industry with intelligence that is timely and actionable would allow industry to better Prevent and Detect scams.

In relation to industry support, FS-ISAC members are specifically interested to learn:

- which Government entity will oversight the reporting portal and/or platform?
- is the provision of intelligence to support industry part of that entity's remit?
- if materials are provided to industry, what are the restrictions on sharing? and
- what feedback on scam reports be provided to industry (e.g. will Government advise on the instigation and/or outcome of any law enforcement investigations, legal actions or other Government-led responses)?

FS-ISAC members would encourage a 'partnership' with the Australian government, that recognises the extent of investment and the need for mutual benefit.

'Appendix B: Singapore examples of Government sharing' sets out a series of overseas strategies for industry and the community that may assist.

Contextual considerations

Data sharing and privacy

FS-ISAC members would be grateful for clarification on how to effectively balance the need to (a) report scams to Government and (b) ensure the privacy of impacted customers. Any insights that Government can provide will facilitate sharing while also minimising risk to customers.

One potential scenario faced by the financial sector is that information linked to the scam being reported is sourced from telecommunications or other sectors.

Industry with reporting obligations would be assisted by legislated protection from privacy breaches where scam information is provided to Government in good faith. Such an approach may also be (a) applied to sharing with other industry bodies and (b) expanded to include cyber threat and money laundering activity.

Legislative and global complexity

FS-ISAC and its Australian members note the significant overlap and interconnection of both cyber threats and money laundering with scams and other forms of financial fraud. A large portion of scams are cyber-enabled and facilitated by cryptocurrency.

While these interdependencies are expected to increase, the proposed Scams Prevention Framework is silent on this matter. A preferable approach to reporting would recognise these complexities and be supported by more contemporary legislation and more integrated Government control frameworks.

Finally, FS-ISAC members with operations in Australia also often have significant operations overseas. This adds a great deal of complexity to reporting, as each nation takes a largely independent view of requirements.

International harmonization of scam reporting requirements – such as in Five Eyes and G7 nations – would reduce the impact of resourcing on industry. Greater international alignment may also improve the ability to share intelligence and collaborate on the detection and disruption of financial scams.

Support for 'upstream' prevention

FS-ISAC and its members note the major impacts of financial scams – both financial and psychological – on the Australian community and the increasing reporting obligations for industry. Addressing scams as far 'upstream' as possible – such as 'smishing' via the telecommunications sector – would provide widespread benefits for the community and industry alike.

However, FS-ISAC members also recognise that scam prevention is not core business for the telecommunications sector. Increased Government support for telecommunications firms (in particular) to help detect and respond to scams at the earliest possible point reduces harm in the most efficient and effective manner.

While challenging and complex to address, scam compounds – which generate large volumes of scams via large-scale operations dedicated to the task – also present a substantial opportunity for prevention. This would help to address not only the financial impacts of scams, but also the associated human trafficking and reinvestment in organised crime.

FS-ISAC are currently reaching out to its domestic and global partners to help the financial sector better identify this activity. This follows the release of our recent intelligence product detailing the operation of scam compounds, such as those in the vicinity of Thailand, Myanmar, Laos and Cambodia.

Contacts

FS-ISAC would welcome the opportunity to discuss these matters further.

Our best point of initial contact is Lisa Jane Young (APAC Intelligence Officer), at ljyoung@fsisac.com.

Alternatively, please contact the Global Intelligence Office at intelligence@fsisac.com

APPENDIX A

Intelligence sharing as core business

The core business of FS-ISAC is to facilitate the sharing of intelligence that is relevant to the security of the global financial sector. This includes intelligence on cyber threats, also fraud and scam activities.

This is facilitated by IntelX, a secure online platform that supports the sharing and consumption of actionable cyber threat intelligence. FS-ISAC supports sharing between members, but also develop its own cyber and fraud intelligence products and briefings.

Two key components of the IntelX platform are:

- 'CONNECT' provides a secure, channel-based environment for members to collaborate with each other and/or with FS-ISAC staff.

- 'SHARE' supports the sharing of tactical, operational and strategic products. Content is tagged and a customizable feed meets specific member needs and interests.

FS-ISAC supports both attributed and non-attributed sharing from members and operates via a Traffic Light Protocol (TLP) system. FS-ISAC also offers a range of briefing and discussions forums, both in person and online.

APPENDIX B

Singapore: Government sharing examples

Provider	Tool	Aimed at
Monetary Authority of Singapore	Investor Alert List	General public
Monetary Authority of Singapore	COSMIC platform	Financial crime in commercial banking
Singapore Government	Shared Responsibility Framework to Combat Phishing Scams (2023)	Financial sector, telecommunications and consumers
National Crime Prevention Council	Scamshield app	General public