18 September 2026

Attorney-General's Department
4 National Circuit
BARTON ACT 2600

Submission to Privacy Reform - Consultation on Exposure Draft Legislation

The Share Fraud Working Group (**SFWG**) was established early 2025 in response to increased share fraud activity - where a person who is not who they claim to be sells shares that do not belong to them and steals the proceeds.

More recently the SFWG has also focussed on share fraud occurring through 'pump and dump' scams - coordinated schemes to pump up share prices, before dumping them at inflated prices.

The SFWG currently meets on a quarterly basis and brings together a broad collection of industry representatives supporting investor shareholdings on Australian equity markets (including across issuers, financial markets, brokers and registries) as well as relevant regulatory agencies, to combat such fraudulent activity by:

- enhancing knowledge and information sharing
- facilitating an uplift in member processes
- advocating for actions requiring support beyond industry members.

I act as Chair of the SFWG, and in that capacity welcome the opportunity to provide feedback on Exposure Draft legislation to modernise and strengthen Australia's privacy laws for the digital age.

The digital age heightens the risk of share fraud, particularly for Australians affected by data breaches whose personal information is now available online and may be used for identity theft.

Shareholdings are also increasingly targeted by sophisticated fraud syndicates, with the tactics used continuing to evolve in complexity and being increasingly difficult to detect and disrupt.

Share fraud risks and privacy law impediments to responding

Share fraud creates a risk of loss by investors from fraudulent actors impersonating individuals who have had their personal identity compromised or hacking their accounts and then stealing their shares or using compromised accounts to 'pump and dump' specific stocks.

It also creates a risk of loss to APP entities, including under statutory warranties and indemnities which require that brokers have authority from the shareholder when effecting share transfers.

To ensure market integrity and investor confidence, industry needs to be able to share intelligence quickly where specific fraud activity is detected in order to disrupt the activity and protect investors by avoiding their shares or cash being sold or moved.

This includes through the sharing of identifying details for fraud victims or fraudulent actors (such as name or phone number held or malicious IP address identified) between persons who may be affected by, or can assist in combatting, the fraud.

The sharing of such information could, for example, allow:

- the broker targeted by the fraudulent actor to cross-check information on suspected compromised accounts (including contact details provided by the fraudulent actor) with details for the fraud victim maintained by another party (e.g. the share registry for the holdings), to:
    - alert if details don't match
    - allow accounts to be red-flagged
    - allow the victim to be contacted.
- the sponsoring broker of the potential fraud victim whose shares are being transferred out to validate the transfer with that victim (where not the broker targeted by the fraudulent actor)
- other brokers to check if fraudulent actors are setting up multiple fraudulent accounts with them using the same information, so as to also put them on notice.

Privacy restrictions are however frequently cited by SFWG members as having a detrimental effect on actions they can take to stop fraudulent activity by restricting their ability to share personal information when a fraud is suspected. This includes where such sharing was otherwise viewed as the right thing to do to help stop movements of shares and cash to avoid or mitigate investor losses.

Support for changes that appropriately address privacy impediments

Accordingly, I am supportive of proposed changes in the Exposure Draft that would help overcome privacy obstacles raised by SFWG members for appropriately sharing information in relation to fraud events.

As set out below, this includes through the reforms:

- addressing a key current roadblock to relying on the existing '*permitted general situation*' exception
- providing scope to consider *benefits* from collecting, using or disclosing information to prevent losses from a fraud on an investor's shareholdings.

Included below is also a suggestion to make clearer the role for considering the *risks* in not sharing information (in addition to the benefits of doing so).

Widening '*permitted general situation*' exception

One of the proposed changes under the privacy reforms addresses a narrowing of the scope of the '*permitted general situation*' exception due to a statement in the Explanatory Memorandum to privacy reforms in 2012, which is cited by the OAIC in its guidance (available here – refer to C.15) as limiting the application of that exception to an entity's '*internal investigations*' about activities within or related to the entity. The example of an '*internal investigation*' provided in the Explanatory Memorandum relates to an internal fraud or breach.

This poses an obvious limitation to reliance on the '*permitted general situation*' exception where the fraudulent actor is a third party that is external to the APP entity, which reflects the typical fraud scenario experienced by SFWG members.

Changes proposed under the privacy reforms to widen the operation of the '*permitted general situation*' exception, so as to apply regardless of whether the person engaging in conduct is internal to the entity or otherwise owes a duty to the entity, are therefore welcomed.

Relevantly also in this context, the entity collecting, using or disclosing personal information may not be the entity targeted by the fraudulent actor, but such actions by the other entity can assist in preventing the fraudulent activity, as indicating in the above examples.

Consideration of '*benefits*' under new '*fair and reasonable in the circumstances*' test

New Privacy Principle 3.2 prescribes matters an entity must consider in determining if collection, use or disclosure of personal information is fair and reasonable in the circumstances, which includes whether the impact or risk of harm to the individual is proportionate to any '*benefits*' to the individual or APP entity from such collection, use or disclosure (paragraph 3.2(f)).

The ability to have regard to *benefits* to the individual or APP entity from collection, use or disclosure of personal information may provide scope to consider the value to them of preventing losses from a fraud on the individual investor's shareholdings, and is therefore welcomed.

Given the *risk* of harm arising from share fraud which the timely sharing of identifying details of fraud victims and fraudulent actors seeks to prevent, it would be helpful if paragraph 3.2(f) also expressly facilitated consideration of any '*risk*' to the individual or APP entity from not collecting, using or disclosing the personal information.

I would welcome the opportunity to discuss these matters further with you.

Kind regards

Con Korkofigas
SFWG Chair