

Issues already with ASIC removal of director address details

17 February 2026 • By Matthew Burgess, View Legal

Matthew Burgess, director at View Legal, has highlighted issues with ASIC's removal of director address details on company extracts purchased through its website.

On 2 February 2026, ASIC confirmed its decision to remove the residential addresses of company officeholders on company extracts purchased through the ASIC website.

In making the announcement, ASIC confirmed it “implemented this change in response to broader privacy and safety concerns, including the potential to access personal information, heightened concerns around personal safety and to reduce the risk of identity theft and cyber crime.”

The regulator also said the change was a “sensible precaution that balances the need to reduce easily accessible personal information while maintaining effective and transparent registers.”

Relevantly, it was confirmed that the change would not remove residential address information entirely from the ASIC website, but rather was “designed to create a barrier at the most widely available access point.” What is, in fact, achieved by the change in approach, however, is questionable from a number of perspectives.

For example, the change does not remove residential address information from documents lodged with ASIC previously, meaning relatively simple (and inexpensive) second-order document searches will still ensure easy access to residential address details.

Nor does the change impact any search conducted historically and retained (e.g. as a saved PDF). Perhaps more concerning, it appears based on searches since the announcement that if the relevant officeholder is a shareholder (or member) of the relevant company, ASIC extracts will continue to disclose the personal residential address details.

In the overwhelming number of situations, officeholders will own shares in at least one company they are a director of. Thus, in a 2-page search, while the address on the first page will be replaced by ASIC with the words “Not available in this ASIC extract,” on the second page, the full residential address will still appear. Furthermore, officeholders will still be required to update residential address details within 28 days of any change. ASIC is yet to develop rules for when these details will be disclosed to third parties such as liquidators, lawyers and other statutory authorities.

It is also unclear how other providers of ASIC company extracts will respond to the ASIC iteration in their approach.

Given that the so-called “barrier” appears at best theoretical, officeholders concerned about disclosure will still practically be required to have a formal suppression of the address approved by ASIC.

Anecdotally, few suppression approvals have been granted historically, with the process involving:

1. Being registered as a silent elector with the Australian Electoral Commission (requiring proof that you believe having your address on the public electoral roll could put you or your family's safety at risk).
2. Separately apply to ASIC for suppression of address details.
3. If approved by ASIC, provide an alternative street address for ASIC records.

Similar issues regarding the confidentiality of private residential address details arise in a range of areas, with court applications an obvious example.

In the decision of *Application of Connelly; The Estate of Nancy Allwood Connelly* [2023] NSWSC 467, the court had to consider whether publishing the residential address of an executor in probate documents posed a genuine risk to safety or privacy.

The applicant argued that disclosure could expose them to harassment or harm from an estranged sibling, and that the address was not essential for the public to understand or verify the probate process. In denying the address suppression request, the decision explored a range of issues (a number of which are likely to be considered relevant to any request to suppress address details with ASIC), including:

- (a) The principle of open justice (that is, the presumption that court proceedings and documents are public).
- (b) Applying a "calculus of risk approach," which requires a court to consider the nature, imminence, and degree of likelihood of harm to the relevant person when determining whether an order is necessary to protect the safety of the person (see *Hogan v Australian Crime Commission* (2010) 240 CLR 651).
- (c) Understanding that if the prospective harm is very severe, then it may be the case that an order would be necessary even if the risk of harm does not go beyond a mere possibility.
- (d) Confirming that compelling evidence of the risks of disclosure had to be provided - thus the belief that a pre-existing psychological condition may be exacerbated or aggravated is generally of itself insufficient for the purposes of establishing that an order is necessary to protect the safety of that person or another person (see *A Lawyer (a pseudonym) v Director of Public Prosecutions NSW; Nationwide News Pty Limited v A Lawyer (a pseudonym)* [2020] NSWSC 1713).
- (e) Where, as here, the evidence of risks was vague in the extreme and amounted to no more than allegations unsupported by any incidents, the appropriate remedy (if issues arose in the future) was a step such as an apprehended personal violence order (a process the court noted as "safe, speedy, inexpensive, and simple, as is reasonably possible.").