14 October 2026

Registry Stakeholder Engagement Team
Australian Securities and Investments Commission
GPO Box 9827
Melbourne Victoria 3001

Submission to Australian Securities and Investments Commission's consultation on *Access to information on the companies register (CP 391)*

Submitted by:
UNSW Tax and Business Advisory Clinic

Executive summary

The UNSW Tax and Business Advisory Clinic (the Clinic) welcomes the opportunity to provide a submission to the Australian Securities and Investments Commission's (ASIC) consultation on Access to information on the Companies Register.

The Clinic supports improved access for vulnerable individuals and community service providers to corporate information. However, this position needs to be balanced with the preservation of privacy and safety for victim-survivors of financial abuse.

Our submission makes the following recommendations:

1. **Improve visibility of actual company control (Question 2).**
   ASIC should design its access framework to accommodate information about ultimate ownership and control as the Government's beneficial ownership reforms progress. Such information reflects the current regulatory, legal and governance environment. This could assist in understanding arrangements where formal appointments do not reflect practical control. Any additional collection and disclosure requirements should include appropriate privacy safeguards.
2. **Protect sensitive personal information through ordinary access settings (Questions 3, 4 & 5).**
   Use year of birth and state and country where those details are made available through general access. Residential addresses should not become generally accessible because a service address has not been lodged, and protection should extend to individual members of proprietary companies. Provide assistance to establish service addresses and restrict fuller personal information to access justified by a specific purpose and demonstrated need.
3. **Distinguish current and historical appointments (Question 4).**

CRICOS Provider Code 00098G

Clarify the proposed officeholder-status field and retain a focus on current officeholders in free extracts. Make previous appointments available through clearly identified historical searches, distinguishing ceased roles from current involvement and preserving access for authorised client assistance.

4. **Use a confirmation indicator without publishing Director ID numbers (Questions 4, 8 and 9).**
   ASIC should clearly explain and test each indicator's meaning and provide safe correction and review processes that preserve the confidentiality of safety concerns. Full Director ID numbers should remain outside both free and paid general access. An indicator is sufficient to communicate that ASIC has obtained the number from ABRS. It should not imply verification of associated personal details, consent to an appointment or control of company affairs. Individuals and appropriately authorised professionals should have a safe pathway to obtain the number.
5. **Clarify and apply redaction consistently (Question 7).**
   ASIC should specify which information fields, and which parts of those fields, will be redacted for each access category, supported by examples. Privacy protections should also address historical documents, including an urgent pathway to restrict sensitive information. Redaction should preserve access to information reasonably necessary for authorised client assistance.
6. **Provide fee-free access for verified community professionals (Question 12).**
   Financial counsellors, community lawyers, community tax practitioners and specialist economic abuse services should have fee-free access to current and historical information reasonably necessary to assist clients, including information about relevant connected entities and officeholders. Access should be supported by verification of organisations and individual users, client authority or another appropriate lawful basis, purpose limitations and audit records. Sensitive information should remain limited to what is necessary for the client matter.
7. **Build safety into representative-access processes (Question 15).**
   Distinguish authority to represent a company from authority to represent an individual. Enable independent advocacy, record and safely revoke authority, and provide prompt human review of disputes while respecting separate statutory access rights. Professional status should not automatically confer access to residential addresses. Protect confidential contact details, provide timely consideration of interim disclosure restrictions, and apply safeguards for use, onward disclosure and suspected misuse. Develop and test these arrangements with frontline community services.

Together, these recommendations seek to preserve useful corporate transparency while embedding Safety by Design and enabling vulnerable individuals to understand and address their affairs.

About Us

The National Tax Clinic program is an Australian Government funded service which provides free tax advice to clients that would otherwise be unable to access such advice due to financial hardship or other vulnerabilities. The UNSW Tax and Business Advisory Clinic was established as part of this program by the University of New South Wales in 2019.

The Clinic exclusively assists vulnerable individuals and small businesses with tax matters. Our casework includes victim-survivors of abuse and individuals affected by coerced or fraudulent directorships, misuse of corporate entities, or arrangements in which another person exercises practical control over company affairs. These clients have been referred to the Clinic by community service partners including financial counsellors and pro-bono legal clinics. The lived experience in Annexure A provides insight into the complexities.

Our Submission

To ensure that our responses to the questions are targeted and highly relevant to our frontline experience, we have provided answers to select questions raised in the consultation paper.

***Question 2* - Are there any information types that should be added, removed, combined or described differently?**

The Clinic supports including information about individuals who ultimately own or exercise significant control over a company, alongside recorded officeholders. Our casework includes individuals formally appointed as directors while another person controls company communications, records and financial decisions. Information about actual control could assist in investigating these arrangements and understanding clients' tax affairs, without itself determining coercion or liability.

We welcome the Government's commitment to a beneficial ownership register for unlisted companies and recommend that ASIC's access framework accommodate this information as the reform progresses. We recognise that additional reporting obligations may require work beyond this consultation.[1] Consistent with Safety by Design, disclosure should identify relevant ownership and control relationships while protecting sensitive personal details. Verified community professionals should have fee-free access to additional information reasonably necessary to assist clients, subject to appropriate safeguards. Overseas approaches offer useful examples of distinguishing information collected from information publicly disclosed.[2]

***Question 3* - Do you agree with the proposal to provide subsets of personal information (i.e. year of birth instead of full date of birth and state and country instead of full residential address)?**

The Clinic supports the proposed subsets for general access, including year of birth instead of full date of birth and state and country instead of full residential address. We agree with the recommendation of Economic Abuse Reference Group (EARG) that these protections should be accompanied by access to fuller information for authorised users where necessary for legitimate verification, investigation and advocacy.

For clients affected by coerced or fraudulent directorships, limited information may be insufficient to establish whether a record relates to them, distinguish individuals with similar names or investigate connected entities. Verified community professionals should therefore have fee-free access to fuller information reasonably necessary to assist with these matters, subject to appropriate authority or another lawful basis.

Authorisation should not automatically provide access to all sensitive details. Access to full birth dates or residential addresses should reflect the specific purpose and why the subset is insufficient, with safeguards for use, onward disclosure and audit. This would preserve meaningful access for client assistance while protecting individuals from unnecessary exposure.

---

[1] Treasury, *Improving transparency of the true owners of companies*, 15 October 2025.

[2] The UK's people with significant control framework protects home addresses supplied as residential addresses from public disclosure. Singapore requires registrable controller information to be lodged with ACRA, but its central register is not publicly accessible: Companies House, *People with significant control (PSCs)*; ACRA, *Filing with the Central Register of Registrable Controllers*.

***Question 4* - Do you agree with the information we propose to make available through free and paid general access? Is there any information that should be restricted?**

The Clinic broadly supports ASIC's proposal to improve access to company information while balancing transparency with individuals' privacy, safety and security. For our clients, occasionally, access can help uncover company involvement arising from coercion or identity misuse. However, general disclosure of personal information may create further risks. We recommend the following refinements.

Director ID numbers

Full Director ID numbers should remain outside both free and paid general access. An indicator confirming that ASIC has obtained the number from ABRS is sufficient to communicate that fact. Its meaning should be clearly explained: receipt does not establish the accuracy of associated personal details or the individual's awareness of, or consent to, a particular appointment.

We recognise the value of tracing individuals across company appointments and encourage ASIC to support that function through arrangements that minimise disclosure of the underlying identifier.

For victim-survivors, an indicator may help identify that a Director ID exists in their name. Individuals and appropriately authorised community professionals should have a safe pathway to obtain the number where needed to understand and address their affairs.

This position is consistent with EARG's concern about disclosure through free and unverified paid access. The Clinic recommends excluding full Director ID numbers from both general-access categories, while preserving appropriately authorised access for client assistance.

Current and former officeholders

We support displaying current officeholders in the free extract, helping users identify who presently holds a recorded role. We seek clarification on whether the proposed "officeholder status" field would also display former officeholders, and how the distinction between current and historical extracts would operate. The reference to current and former names does not clearly resolve whether ceased appointments would be included.

The Clinic recommends that the free extract focus on current officeholders, with previous appointments available through a clearly identified historical search. Historical information remains important for investigating coerced directorships and understanding liabilities. It should remain accessible to authorised community professionals assisting clients, with former roles and cessation dates clearly distinguished from current involvement.

Residential addresses of individual members

The proposed paid general-access category includes the usual name and address of other officers or members. For proprietary companies, we recommend restricting individual members' residential addresses from general access, including paid extracts, while preserving useful information about ownership and shareholdings.

An individual may be both a director and a shareholder. Restricting their address in the officeholder record would provide incomplete protection if the same residential address remained available through the member record. Consistent protection across these roles would strengthen the proposed privacy safeguards.

Where geographical information is needed, it should be limited to state and country. An appropriate service address should be used where contact details are required. Fuller information should remain available through an appropriately restricted pathway where necessary for a legitimate purpose, subject to verification, safeguards for use and onward disclosure, and applicable suppression arrangements. These protections would preserve access needed for client assistance and investigation while reducing unnecessary exposure of personal information.

***Question 5* - Do you agree with the proposed approach to making residential addresses available for general access from 1 August 2028 if a service address has not been lodged with ASIC?**

We do not support making an officeholder's residential address generally accessible solely because a service address has not been lodged. This would make privacy protection depend on an administrative step that an excluded or coerced officeholder may be unable to take.

For individuals affected by coerced or fraudulent directorships, this omission may reflect lack of knowledge, access or control.

Consistent with Safety by Design, where residential locality is disclosed through general access, it should be limited to state, with assistance available to establish a service address. Full residential addresses should remain accessible only through a restricted pathway where necessary for a legitimate purpose, subject to appropriate safeguards.

***Question 7* - Will redacted copies of documents that have been lodged with ASIC be sufficient for the needs of general and business users?**

The Clinic supports redacted documents as a means of balancing access to useful company information with privacy and safety. Whether they are sufficient will depend on what is withheld and the user's access entitlement.

ASIC should clarify which information fields, and which parts of those fields, will be redacted for each access category. Sample documents showing the treatment of residential addresses, birth details and Director ID numbers would help users assess whether the remaining information meets their needs.

For verified community professionals, redaction should not prevent access to information reasonably necessary to assist a client, including investigating coerced directorships or entity misuse. A fee-free, appropriately authorised pathway should enable access to necessary underlying information, with safeguards for sensitive details belonging to other individuals.

ASIC should also address sensitive information in documents lodged before 1 July 2027, including through an urgent redaction pathway. Otherwise, historical documents could undermine the protections applied to newer records.

***Question 8* - Do you agree with our proposal to publish new display flags or indicators, such as director ID confirmation and overdue annual review status?**

The Clinic supports factual display flags that help users interpret register information without unnecessarily disclosing personal details.

For Director ID confirmation, the indicator should state that ASIC has obtained the individual's Director ID number from ABRS. It should not imply that ASIC has verified the accuracy of associated personal details, the individual's consent to a particular appointment or their practical control of company affairs. This distinction is particularly important for individuals affected by coerced or fraudulent directorships.

ASIC should explain what triggers each indicator, when it is updated and how errors can be corrected. Company-level Director ID indicators should distinguish between receipt for some and all directors. An overdue annual review indicator should identify the outstanding obligation without implying misconduct by an individual officeholder.

These explanations should appear alongside the flags and be tested with register users and frontline community services before implementation.

***Question 9* - Are the proposed flags useful for people dealing with companies? Are there any risks or unintended consequences?**

The Clinic considers the proposed flags useful for due diligence, provided users understand their meaning and limitations. Lily's experience (Annexure A) illustrates how identity-related processes may appear complete even when another person controls communications and authentication. A positive Director ID flag could therefore be misunderstood as evidence that an individual knowingly accepted an appointment or controls company affairs.

ASIC should explain the circumstances in which confirmation may be absent, including any pending or transitional states, so users do not automatically infer deliberate non-compliance. Similarly, an overdue annual review indicator should not imply misconduct by an individual officeholder.

A safe process should allow individuals and authorised representatives to challenge information underlying a flag. ASIC should explain who reviews concerns, how the display is managed during review and how corrections are reflected in register outputs.

Where identity misuse or coercion is raised, interim handling should consider safety and procedural fairness. A public notice that a record is disputed or under review could alert a perpetrator or lead to adverse inferences. Raising a safety concern should therefore not automatically trigger a public indicator or disclosure of that concern.

***Question 12* - Are there other business users that should have access to more companies register information? Why does that group need access?**

We welcome ASIC's recognition of community advocates within the proposed company-access arrangements. The Clinic supports EARG's recommendations 12 and 13 for an express, fee-free access pathway for verified community professionals, including financial counsellors, community lawyers, community tax practitioners and specialist economic abuse services. Access to information about a client's own company is valuable but may not be sufficient to understand their circumstances. In matters involving coerced or fraudulent directorships and entity misuse, relevant information may concern previous appointments, connected companies or other officeholders. A client may have no current formal role in an entity whose records are relevant to understanding their exposure. Access should therefore extend to current and historical information reasonably required to investigate and resolve the client's matter.

For the Clinic, this information can assist in identifying recorded company involvement, reconstructing appointment timelines and understanding relationships between entities relevant to a client's tax position. Fee-free access would also support the community services that refer clients to us, helping them identify company involvement and obtain appropriate assistance at an earlier stage.

This access should be supported by verification of eligible organisations and individual users, documented client authority or another appropriate lawful basis, purpose limitations and audit records.

Searches of connected entities should be linked to the client matter without requiring the client to hold an office in every entity searched. Access to sensitive personal information should remain limited to what is reasonably necessary for that purpose.

These arrangements would complement privacy protections by enabling accountable access for client assistance while maintaining appropriate restrictions on public disclosure.

***Question 15* - What safeguards should we put in place for access to company data by company representatives, including company agents, legal representatives, community legal centres, auditors, liquidators and external administrators?**

We welcome ASIC's recognition of representatives engaged by individual officeholders, including community advocates, and its proposed verification of role and authority. These arrangements could help the Clinic's clients obtain records needed to understand their company involvement and tax position. Access processes should clearly distinguish authority to represent a company from authority to represent an individual whose interests may differ from those of the company or its other officeholders.

An individual should be able to authorise an independent advocate without approval from the company's existing agent or another director. Access should reflect the authority granted and the individual's entitlement. Information about relevant connected entities should be accessible where separately permitted under the access framework. ASIC should record the source, scope and duration of authority and provide a safe way to withdraw it. Disputed authority should receive prompt human review, with clear interim arrangements that respect separate statutory access rights.

Professional status should not automatically confer access to sensitive personal information. A legal practitioner may act for a perpetrator of abuse, creating a risk if a victim-survivor's residential address is disclosed to the practitioner or passed to their client. Access should depend on why the particular information is necessary. Where a service address would meet the purpose, the residential address should remain restricted. Where fuller access is necessary, safeguards should govern use and onward disclosure while accommodating lawful service and other legal obligations.

ASIC's proposed hidden-information arrangements provide an important foundation. Consistent with safety by design, ordinary access settings should also protect individuals who have not sought suppression or disclosed abuse. Supplying safe contact details to regain access or obtain assistance should not inadvertently expose those details to another officeholder or representative. A confidential contact channel and timely assessment of interim disclosure restrictions would help address this risk.

We encourage ASIC to develop and test these safeguards with frontline community services. Verification and access processes should be practical for authorised client assistance, supported by audit records and review of suspected misuse. This would preserve the benefits of professional access while reducing the risk that those same pathways expose clients to further harm.

Conclusion

The Clinic welcomes ASIC's work to improve the accessibility and usefulness of the companies register. For individuals affected by financial abuse, coerced directorships or entity misuse, access to corporate information can be an important step towards understanding their circumstances and addressing their tax affairs.

The proposed framework should combine useful public information with fee-free, accountable access for authorised community professionals. Clear indicators, proportionate disclosure and safe review processes would help users interpret records accurately while protecting sensitive personal information.

Embedding Safety by Design in ordinary access settings would extend these protections to individuals who have not yet identified the misuse of their information or sought assistance. The Clinic encourages ASIC to develop and test these arrangements with frontline community services so that improved transparency also supports practical, safe access for vulnerable individuals.

We appreciate the opportunity to contribute and to stand alongside EARG and other sector partners. We would welcome the chance to participate in further discussions, pilots or user testing as reforms are refined and implemented, and we are happy to provide additional case examples or technical input from our tax and DFV-related work.

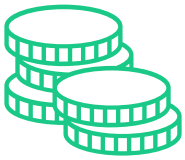
If you have any questions or concerns, please contact me directly on m.madhvi@unsw.edu.au

Acknowledgments

We are grateful for the support and guidance of the following frontline Clinic supervisors in preparation of this submission David Stone, Helen Lam, Annette Tasker, Tony Martins and Jonathon Dorse.

We also gratefully acknowledge the contribution of our Clinic students, whose commitment to supporting financially vulnerable clients is integral to the Clinic's work. We thank our research student, Jerry Weijie Chou, for his assistance and contribution to this submission.

Annexure A – Client Case Study



Lily's ex-husband compromised her tax file number and accessed and operated her tax account without her knowledge or consent. He lodged returns declaring income she had not received, claimed refunds in her name and failed to declare capital gains arising from the sale of two jointly held properties.

He also made Lily a director of three companies without her knowledge. During their relationship, he routinely required her to sign documents without explanation and impersonated her through DocuSign. He controlled email addresses in her name and used them for authentication and electronic signatures, including in director ID and company-related processes. Lily had no access to these accounts or the documents signed in her name and did not know their contents.

Lily only became aware of her directorship role after the Director Penalty Notices (DPNs) were issued to her by the ATO. When the businesses failed, Lily was left as the last recorded director and struggled to obtain basic information about how debts had arisen. She had never communicated with the companies' accountant or authorised them to act for her. Lily's experience demonstrates why a recorded appointment, an electronic signature or the existence of a Director ID does not, by itself, establish informed participation or practical control. It supports safe, independent access to relevant records and careful handling of potentially compromised contact details. It also illustrates the importance of explaining that ASIC's receipt of a Director ID from ABRS does not establish the individual's awareness of, or consent to, a particular appointment.