Law Council
OF AUSTRALIA

Office of the President

11 December 2024

Ms Melissa Harris PSM
Chair, Australian Registrars' National Electronic Conveyancing Council
C/o GPO Box 527
MELBOURNE VICTORIA 3001

By email: chair@arnecc.gov.au

Dear Ms Harris

Security-related obligations under the electronic conveyancing regulatory framework

The Law Council welcomes the opportunity to provide feedback in response to the Discussion Paper, *Security-related obligations under the electronic conveyancing regulatory framework*, published by the Australian Registrars' National Conveyancing Council (**ARNECC**) in October 2024.

Our input is focussed on the security obligations of subscribers, such as solicitors, under the Model Participation Rules (**MPR**), and the security obligations of Electronic Lodgement Network Operators (**ELNOs**), under the Model Operating Requirements (**MOR**). This submission has been prepared with the assistance of the Law Society of New South Wales and the Queensland Law Society with input from our National Electronic Conveyancing System Committee.

Security policies for subscribers and monitoring compliance

The Law Council welcomes appropriate measures to improve the safety and security of eConveyancing transactions. However, in our view, a multi-ELNO environment requires a universal standard approach to streamline requirements and minimise any potential interoperability issues arising from different security requirements.

In our view, the prescription of minimum security standards should not remain with the ELNOs, but is a matter that should be regulated by ARNECC. To have ELNOs prescribing different security standards through their ELNO subscriber security policies is not an appropriately robust approach.

We therefore do not support the first approach outlined on page 5, requiring ELNOs to perform sampled assessments of subscriber' compliance with the ELNOs subscriber security policy.

Consistent with our view endorsing a greater role for ARNECC in prescribing minimum security standards, we support the second possible approach on page 5 - the stipulation of an established cyber security framework or set of agreed standards in the MPR. The challenge then becomes designating an appropriate framework or standard.

In our view, such a framework or standard, must be:

- publicly and freely accessible;

- appropriate for implementation across the range in size of law firms in Australia, particularly noting the prevalence of small law firms; and
- accompanied by communication and education resources.

We also note that any such framework or standard will need to reflect the proposed changes to the *Privacy Act 1988* (Cth), requiring reasonable steps to protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure, as required under Australian Privacy Principle 11, and must include 'technical and organisational measures'.[1] We note that, as at the date of this letter, these measures are not yet law or defined by the proposed legislation.

We further note that the Victorian Legal Services Board and Commissioner has published 'Minimum Cybersecurity Expectations'[2] for Victorian solicitors, which may be of interest to ARNECC as an example of a set of agreed standards.

As an alternative, consideration could be given to the following options:

- that the MPR continues to articulate the most important controls in the context of users engaging with ELNOs;
- to allow greater flexibility and consultation, it may be more appropriate for these measures to be isolated in a security schedule to the Rules that can be updated on a more regular basis; and
- subscribers should have the opportunity to demonstrate compliance with baseline security by certification under an appropriate Industry standard, but use of a particular standard not be mandated.

Appropriate alternative standards for non-mandatory adoption

The Queensland Law Society has also pointed to the emerging SMB 1001-2025[3] standard as a possible starting point for consideration. This standard is designed for small to medium enterprises and is aligned with both NIST, CSF 2.0 and the Essential 8. Once an organisation outgrows it, the control measures specified at the highest tier of the maturity model provide a strong basis for subsequent ISO-27001 compliance.

A certification program for lower maturity tiers under SMB 1001-2025 is available at reasonable cost, which would be a useful and significantly cheaper alternative to an audit program.

The Queensland Law Society advises that it is in discussions with the publishers of the standard to design an industry-specific overlay appropriate to small and medium-sized legal practices. The overlay will be designed to capture the additional controls required by various stakeholders such as insurers, courts and other gateway networks including those currently required by the MPR. It will also be accompanied by supporting resources setting out how the controls may be implemented.

Multi-factor authentication

For most users, the adoption of an appropriate Multi-factor authentication (**MFA**) regime is a sensible security measure. However, caution is required before mandating a particular form of security if this would have the effect of freezing technology at a particular point of time.

[1] Privacy and Other Legislation Amendment Bill 2024, Schedule 1, Part 5, section 34 (first reading) <www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7249>.
[2] Victorian Legal Services Board and Commissioner, *Minimum Cybersecurity Expectations*, last updated 16 August 2024 <https://lsbc.vic.gov.au/lawyers/practising-law/cybersecurity/minimum-cybersecurity-expectations>.
[3] See <http://dsi.org/smbb1001>.

We support the current requirement for MFA to log into an Electronic Lodgment Network (**ELN**). However, we do not support mandating any further requirements for MFA in connection with Virtual Private Networks, administrative and email accounts, as set out on page 7 of the Discussion Paper. There is no direct link from a subscriber's email account to an ELN, and any of the email notifications from the ELN contain de-identified data only. While these systems indirectly support the eConveyancing process, it is not appropriate, in our view, for ARNECC to be regulating these systems.

We understand the concerns in relation to business email compromise and note that mitigation strategies are being adopted by the major banks that should help reduce it, including verification of account details. The use of PayID and OSKO automatically include real-time payee identification and verification, and are to be encouraged. Additionally, solicitors now commonly explain to their clients or have as standard text in their emails, that clients should confirm any payment instructions by telephone before proceeding. In our view, education and awareness for both solicitors and their clients are critical in combatting business email compromise. A more reliable approach would be for government to sponsor a public key lookup table, as ubiquitous as the Domain Name System, to enable all communications to be signed and encrypted for the intended recipient. Individuals can already do this by simply sharing their public key in advance with trusted addressees.

The Discussion Paper also proposes as an alternative on page 7, that the MOR stipulate that an ELNO's subscriber security policy must include a requirement that subscribers implement MFA for all remote access. We assume remote access means any situation in which the solicitor is not using the firm's server, but this requires clarification. We do not think that it is appropriate for ARNECC or the ELNOs to be mandating the use of an MFA for all remote access as a requirement of conducting eConveyancing.

There are varying degrees of adoption of MFA in law firms already, however the implementation costs of stipulating any increased requirement in relation to MFA are likely to be significant and too onerous, particularly for smaller firms. Furthermore, the expansion of the Federal Government's myID (formerly myGovID) for broader identity verification purposes needs to be accommodated if not adopted (see further discussion below on the Digital ID program more generally).

Verification of Identity Standard and reasonable steps

One of the options under consideration in the Discussion paper is to require subscribers to apply the ARNECC Verification of Identify (**VOI**) Standard in all circumstances and to remove the option to take other reasonable steps.

The VOI Standard has existed since the MPR was first issued in April 2013. The concept of taking reasonable steps to identify a client, and the availability of a safe harbour through application of the VOI Standard, have become a daily part of conveyancing practice. We regard the current approach to VOI, which provides these two pathways, as striking the right balance between flexibility and robustness of process.

While solicitors are encouraged to use an in-person verification process as standard,[4] there are circumstances in which alternative verification is both low risk and more appropriate. This is particularly important in jurisdictions serving a wide geographical area where a significant proportion of clients have difficulty attending their solicitor's physical office or accessing in-person verification options.

[4] See, for example, guidance on the QLS website, <https://www.qls.com.au/Practice-Support-Tips/Verification-of-client-identity>.

Particularly in regional areas, solicitor-client relationships may be decades or generations old, with the identity of the client being well known to the solicitor. In such circumstances the risk of impersonation is low[5] and the cost and disruption of forcing physical attendance of all parties for VOI is significant.

Mandating in-person VOI would also inevitably impede commercial development of appropriate alternative technologies. We recommend that the reasonable steps option for VOI be maintained, and a legal practitioner should be able to exercise his or her professional judgment to assess the appropriate method of doing so in all the circumstances of the case. To further support this position, it is suggested that ARNECC should provide guidance on what might constitute 'reasonable steps' to assist practitioners in those cases.

While we are supportive of the role the VOI Standard currently plays, our opposition to mandating the VOI Standard in all instances, or for certain conveyancing transactions (as outlined in the Discussion Paper), is further detailed below.

VOI Standard in all instances

As the Discussion Paper acknowledges in the last paragraph on page 10, mandating use of the VOI Standard in all instances would result in no flexibility for the carrying out of VOI other than through a face-to-face meeting. We agree with the conclusion in the Discussion Paper that this may cause issues for clients based in regional or remote communities, or clients based overseas. It may also cause issues for elderly clients, clients with mobility issues, or immigrants who may be unable to satisfy the requirements of the VOI standards. Retaining the reasonable steps option also allows VOI to be conducted over audio visual link in appropriate circumstances, and we note this flexibility was critical during the COVID-19 pandemic.

More generally, as alluded to on page 11 of the Discussion Paper, the reasonable steps option allows subscribers to take advantage of digital VOI options. Retaining the reasonable steps option will allow subscribers to incorporate use of the Digital ID technology as soon as it is available, and indeed any future technological advances in VOI. The Discussion Paper notes the development of the Digital ID framework, and that ARNECC will consider the new Digital ID framework closer to implementation. We support that approach and suggest that in the intervening period, no changes should be made to the current VOI framework under the MPR.

The Discussion Paper suggests that using the services of an Identity Agent to carry out VOI in accordance with the VOI Standard may offer some flexibility, but such services are not always readily available in regional or remote communities.

In our view, a proposal to mandate the use of the VOI Standard in all instances overlooks the professional judgment of solicitors when conducting an eConveyancing transaction. Using reasonable steps to verify the identity of a client is an extension of the very basic principle of knowing your client.

We are also concerned with other practical implications of mandating the VOI Standard in all instances. For example, if the transacting party is a publicly listed company, applying the VOI Standard to office bearers is unworkable and disregards the reality of commercial practice. Another example where applying the VOI Standard is unworkable includes when the transacting party is the Crown or a local Council. The current requirement to take reasonable steps adequately addresses the question of appropriate identification by allowing the practitioner to determine an appropriate identification process, having regard to the nature of the client.

[5] Provided that the solicitor establishes real-time communication with all clients rather than relying solely on email or recorded messages.

The current approach to VOI also provides a degree of flexibility where the location or circumstances of the client make the application of the VOI Standard difficult. For example, clients who have lost all their identity documents in a natural disaster, or clients in remote communities who may not have sufficient identity documents. A focus on reasonable steps to verify identity in the circumstances, rather than the rigid application of the VOI Standard is entirely appropriate in our view in these and similar circumstances.

An increasingly problematic aspect of the VOI Standard is the requirement to retain copies of the identity documents provided by the client.[6] If the VOI Standard was to be mandated in all instances, this would create a significant issue for clients who are uncomfortable with the retention of copies of their identity documents. In the profession's experience, in light of recent data breaches, clients are understandably more reluctant to permit their solicitor to retain copies of their identity documentation. In these situations, a solicitor might instead adopt a reasonable steps approach, and make a file note of the identification documents presented and verified, rather than taking a copy of the identification documents. The critical issue is the sighting of the identification documents, and *verification* that the documents are those of the client, retention of copies of the identity documents is merely one form of evidence, with attendant security risks.

Mandating the VOI Standard to be used in all instances would increase the retention of copies of client identification documents by law firms and may increase the risk of being targeted by hackers. We note that utilising the Digital ID framework will reduce the risks associated with law firms holding identity data, as would facilitating legal practitioners' use of the Document Verification Service[7].

VOI Standard in certain conveyancing transactions

We do not support requiring subscribers to use the VOI Standard in 'certain conveyancing transaction types considered to be of increased risk' as set out on page 11 of the Discussion Paper. We note that these types of policy considerations potentially overlap with measures to further regulate solicitors under the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024*.[8] Once operational, the Anti-Money Laundering and Counter-Terrorism Financing (**AML/CTF**) framework will contain customer due diligence or 'know your client' obligations upon solicitors for designated services which includes the provision of real estate services.

We suggest it would be undesirable for ARNECC to adopt a more prescriptive approach to VOI at this stage. In our view, the VOI framework should remain flexible, and ideally, harmonisation sought between the steps a solicitor must take to verify the identity of their client under both the AML/CTF framework and the MPR framework.

It is suggested that any changes to the MPR should be delayed until the AML/CTF rules and regulations are published by AUSTRAC. It would be inefficient and costly for legal practitioners if the ARNECC VOI requirements are to be duplicated or even inconsistent with the final approach to be required by AUSTRAC.

Supporting evidence obligations in the MPR

While retention of client documents for seven years or longer is the default position with respect to legal files, it should not be assumed that the same must apply to honeypot data such as VOI records.

[6] Verification of Identity Standard, Model Participation Rules, Paragraph 3.3(b), Schedule 8 <www.arnecc.gov.au/wp-content/uploads/2024/01/Model-Participation-Rules-Version-7-Clean.pdf>.
[7] The convoluted arrangements presently in place are difficult for the majority of small firms to utilise: <https://www.idmatch.gov.au/organisations/business-user>.
[8] The changes made by this new legislation will take effect in March 2026.

It is questionable whether the benefit of keeping copies (as opposed to ensuring that the originals or certified copies have been sighted and verified) justifies the risk to consumers of capturing, transmitting and storing hundreds of thousands, and potentially millions, of sets of sensitive personal identity documents for nearly a decade. It is inevitable that significant numbers of these will be compromised, especially if the entities holding the data have inadequate defences against increasingly sophisticated hacking techniques.

A certificate from a solicitor stating that a passport with a specific number was sighted and appeared to match the person presenting it has nearly the same utility as subsequent evidence as a scanned copy of the document itself. It would be prudent to consult with the Australian Information Commissioner prior to continuing the practice of wholesale ID scanning.

While acknowledging the above concerns, at this stage we continue to generally support retaining the current obligation to retain supporting evidence for 'at least seven years from the date of Lodgment' under MPR 6.6. In our view, the period of seven years is appropriate given that a solicitor may be asked for evidence as part of a compliance examination, or for provision to a Court if a dispute arises. We further note that the seven-year period of retention mirrors a solicitor's retention obligations under Rule 14.2 of the *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015*,[9] which apply in New South Wales, Victoria and Western Australia.[10]

However, we note that a subscriber can be required to submit to a compliance examination at any time post an eConveyancing transaction, that is, potentially beyond a seven-year time period, such that in practice, law firms may retain supporting evidence including identity documents from the VOI Standard indefinitely. Further, the use of the terminology in MPR 6.6. of '*at least'* seven years provides a minimum standard and supports, if the subscriber determines, a longer retention period of supporting evidence, potentially indefinitely. We suggest that consideration could be given to amending the provisions regarding compliance examinations under the *Electronic Conveyancing National Law*,[11] to introduce a time limit on the ability of the Registrar to conduct a compliance examination. This may assist to reduce the retention of identity documentation by subscribers.

We note the comments in the final paragraph on page 12 of the Discussion Paper, about potential alternatives to storing personal information, particularly the storage of copies of identity documentation required under the VOI Standard. As noted above, this is an area of concern for both clients and lawyers. The Digital ID framework will reduce the need to take copies of identity documentation from clients when using reasonable steps to verify the identity of clients, and further reduce the need to indefinitely retain these copies of identity documents as supporting evidence in contemplation of a future compliance examination, which will be welcome. Awareness and education about safe ways to store personal information is also critical to reducing this security risk.

Further alternative options for document retention include allowing the certifying party to upload supporting documents to the ELN, rather than having to retain it on their system. Alternatively, it may be possible to implement a hybrid approach where metadata or anonymised records are retained for seven years, while sensitive personal information is securely deleted after a shorter period (e.g. three years). Mandatory encryption for stored data could also be introduced to mitigate such risks.

[9] Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015 (NSW), <https://legislation.nsw.gov.au/view/html/inforce/current/sl-2015-0244>.
[10] Seven years is generally regarded as sufficient to preserve documents at least for the duration of the standard six-year statute of limitations.
[11] Electronic Conveyancing National Law 2012 (NSW), Part 3, Division 5, Compliance examinations <https://legislation.nsw.gov.au/view/html/inforce/current/act-2012-88a#pt.3-div.5>.

Contact

The Law Council would be pleased to discuss the matters raised in this letter. Please contact Nathan MacDonald, Deputy General Manager of Policy at nathan.macdonald@lawcouncil.au, or on (02) 6246 3721 in the first instance.

Yours sincerely



Greg McIntyre SC
President