THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PLC:BMgl281124

28 November 2024

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
Braddon ACT 2612

By email: nathan.macdonald@lawcouncil.au

Dear Dr Popple,

Consultation on MPR and MOR security related matters

Thank you for the opportunity to provide input on the Discussion Paper, *Security-related obligations under the electronic conveyancing regulatory framework*, for a submission to the Australian Registrars' National Electronic Conveyancing Council (**ARNECC**). The Law Society's Property Law and Privacy and Data Law Committees contributed to this submission.

We note that the Discussion Paper appropriately includes discussion of the security obligations of Subscribers, such as solicitors, under the Model Participation Rules (**MPR**), and the security obligations of Electronic Lodgment Network Operators (**ELNOs**), under the Model Operating Requirements (**MOR**).

As a general comment, we suggest that before making any significant change to security obligations of Subscribers, a cost-benefit analysis should be undertaken. It would also be helpful for stakeholders to see data on the number of compromised eConveyancing transactions and the cause of the compromise. While we understand the sensitivity of some of this information, some broad indications of scale and cause would be helpful in determining whether any changes are warranted.

1. Security policies for Subscribers and monitoring compliance

In our view, given the multi-ELNO environment that now exists, the prescription of minimum security standards should not remain with the ELNOs, but is a matter that should be regulated by ARNECC. To have two (or more) ELNOs potentially prescribing different security standards through their ELNO Subscriber security policies does not seem an appropriately robust approach. 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.

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

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au

T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au

Law Council OF AUSTRALIA
CONSTITUENT BODY

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), that is, require 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 of the date of this letter these measures are not yet law or defined by the proposed legislation.

We 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.

2. Multi-Factor Authentication (MFA)

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 that should help reduce it, including verification of account details by financial institutions such as Westpac and the Commonwealth Bank. 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.

The Discussion Paper also proposes as an alternative on page 7, that the MOR stipulate that an ELNOs' 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.

---

[1] Privacy and Other Legislation Amendment Bill 2024, Schedule 1, Part 5, section 34 (first reading) https://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.

There are varying degrees of adoption of MFA in law firms already, but the implementation costs of stipulating any increased requirement in relation to MFA are likely to be significant and too onerous, particularly for small firms.

3. Verification of Identity Standard and reasonable steps

We note that the Verification of Identity Standard (**VOI Standard**) under Schedule 8 of the MPR has existed since the MPR 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 we are supportive of the role the VOI Standard currently plays, we do not support mandating that the VOI Standard be used in all instances, or used in certain conveyancing transactions. Our response to these two possible approaches, outlined on pages 10 and 11 of the Discussion Paper, is 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 in the Discussion Paper on page 11, 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.

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. A "one size fits all" approach of routinely requiring the VOI Standard to be applied is not appropriate.

An increasingly problematic aspect of the VOI Standard is the requirement to retain copies of the identity documents provided by the client.[3] 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 our members' 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.

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 the current proposal to regulate solicitors under the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024.[4] The Anti-Money Laundering and Counter-Terrorism Financing (**AML/CTF**) reforms, if passed in their current form, will commence on 1 July 2026. The AML/CTF regime 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 at this stage for ARNECC to adopt a more prescriptive approach to VOI. 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. We suggest that it may be appropriate for ARNECC to further consider the approach to VOI under the MPR framework once the Digital ID and AML/CTF frameworks have been implemented.

4. Supporting evidence obligations in the MPR

We 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*

[3] Verification of Identity Standard, Model Participation Rules, Paragraph 3.3(b), Schedule 8 https://www.arnecc.gov.au/wp-content/uploads/2024/01/Model-Participation-Rules-Version-7-Clean.pdf.
[4] Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7243.

Profession Uniform Law Australian Solicitors' Conduct Rules 2015,[5] which apply in New South Wales, Victoria and Western Australia.

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*,[6] 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, 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.

Please contact Gabrielle Lea, Senior Policy Lawyer, on (02) 9926 0375 or gabrielle.lea@lawsociety.com.au if you have any questions in relation to this letter.

Yours sincerely,

Brett McGrath
President

[5] *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015* (NSW), https://legislation.nsw.gov.au/view/html/inforce/current/sl-2015-0244.
[6] *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