ABN 92 140 677 792
Property Exchange Australia Ltd

Continuing Professional Development Review
Victorian Legal Services Board and Commissioner

By email: CPDreview@lsbc.vic.gov.au

17 July 2020

Dear Reviewers

Review into Continuing Professional Development

PEXA is grateful for the opportunity to provide feedback to this Review into Continuing Professional Development (CPD) for Victorian legal practitioners and wholly supports the Victorian Legal Services Board and Commissioner's (VLSB+C) objective to achieve meaningful, relevant and accessible learning and development opportunities for all Victorian lawyers.

About PEXA

PEXA was formed in 2010 to fulfil the Council of Australian Governments' initiative to deliver a single national electronic system for the settlement of real property transactions for the Australian property industry. We provide an electronic conveyancing (eConveyancing) solution to our members, including lawyers and financial institutions, that enables them to lodge documents with Land Registries and complete financial settlements electronically, rather than having to attend a physical settlement.

PEXA's comments on the Review

On the basis of our experience as an established Electronic Lodgement Network Operator in five, soon to be six, jurisdictions across Australia, our comments focus on the profession's increasing adoption of new technology and digital platforms such as PEXA's, and the desirability that all practitioners are aware of and implement good cyber security practices, policies and culture informed by appropriate cyber security training. While we do not advocate that cyber security training be made mandatory, we do strongly recommend that the VLSB+C gives serious consideration as to whether it would be appropriate and timely to do so, including for the reasons we set out on the following pages.

More generally, PEXA supports the continued delivery of CPD training via a range of different methods such as webinars, conferences, workshops, discussion groups and more. We believe each of these options can facilitate effective learning and development opportunities for lawyers across a range of subject areas and we believe this flexibility should be retained to allow practitioners to choose what suits them best at any point in time.

We also suggest, if the 'points scheme' is to be retained, that the VLSB+C consider publishing and promoting additional guidance for practitioners around the nature of these requirements at a local (Victorian) level including as to the four compulsory subject fields. From PEXA's experience in delivering practitioner training, there has been some confusion around the activities that can be

counted towards a practitioner's annual CPD unit requirements and an overemphasis on the points that are to be attained rather than the learning opportunities at hand. We also note that PEXA is regularly asked for 'CPD certificates' for webinars and other PEXA-run events, whereas the evidence that solicitors must keep in support of the activities they have undertaken may take many forms and need not be certificates issued by training providers.

Cyber security training for lawyers

Cyber security is essential in maintaining the safety and security of financial settlement arrangements for online property transactions and is vital to ensuring that Australian consumers have trust and confidence in the integrity of the eConveyancing industry. Cyber crime is a moving, active risk against which cyber security provides a continuous and informed counter. To the extent that there may be practitioners who require increased levels of understanding and competence in the eConveyancing operating environment, the establishment of mandatory industry requirements to further bolster standards for risk assessment, management and controls applicable to their relative market participations and practice areas may be useful to achieve or contribute to this level of knowledge.

eConveyancing must be a safe and effective system upon which consumers, practitioners, financial institutions, governments, regulators and the wider community depend for trust, confidence, security and certainty with land transactions. Effective cyber security practices and broad awareness among practitioners are vital to ensure that this occurs and to safeguard property transactions for consumers. We discuss in some detail below the topics and risk areas we consider are important for practitioners who undertake transactions on an eConveyancing platform to be aware of.

Review of the IGA for an eConveyancing National Law

The Review of the Inter-Governmental Agreement for an Electronic Conveyancing National Law (the IGA Review) completed last year examined a range of issues relevant to cyber security in the eConveyancing context, identifying several options for improvement and further consideration.

We have set out below some of the analysis and conclusions reached in the IGA Review Final Report, which we consider may assist the VLSB+C in its examination of the skills required of practitioners today and into the future:

> *Cybersecurity risks will need to be carefully monitored and risk mitigation strategies developed given the attractiveness of the large value payments handled in eConveyancing, and the criticality of those payments to individual homeowners. (paragraph 3.8)*
>
> *For the eConveyancing system, cyber threats have the potential for material consequences including:*
>
> - *Land information – unauthorised modification compromising titles integrity*
> - *Financial information – unauthorised modification resulting in misdirection of funds and financial loss*
> - *Transaction – disruption and delay of settlement resulting in emotional distress and financial loss*

- *Personal information – misuse, interference, loss, unauthorised access, modification or disclosure breaching individual's privacy (paragraph 4.189)*

Subscriber security practices have not developed sufficiently for the eConveyancing environment with its high value payments eg attempts to inject fraudulent destination bank account details via BEC have occurred. (paragraph 4.201)

There is a lack of system wide focus on cybersecurity and no skilled national resources to address the issue. While there are security obligations identified in the Model Participation Rules, there are no identified security improvement programs for subscribers. We understand there is a significant gap in ongoing education in cyber security for smaller practitioners (para 4.202)

Options for improvement

Consider developing a formal consultative option with relevant cybersecurity experts including federal government, private sector, practitioner regulators, insurers and professional bodies to enable development of strategies to counter threats.

Consider whether future certification of practitioners should require a reasonable level of competence in operating in an electronic environment and a good understanding of cybersecurity.

All stakeholders that commented on this option supported it.

(page 17, Option 7)

Option for further consideration

Consider requiring information security certification for practitioners eg professional development credits via the Victorian Legal Services Board (paragraph 4.205).

Additional information can be found in the IGA Review Final Report via the www.arnecc.gov.au.

Cyber security risks and the COVID-19 pandemic

The recent shift to working remotely has the potential to increase vulnerability to cyber crime, particularly where security protections afforded to system users typically rely upon connection to their organisation's central network. The elements considered to impact the security risk profile of electronic conveyancing are described further below.

Systems Security

While the architecture of PEXA's Electronic Lodgment Network (ELN) itself is not compromised by the move to remote working, the shift does have the potential to adjust how access to the ELN platform is managed, thereby impacting the security risk profile for practitioner firms and their employees. In consideration of this, PEXA has been providing members with guidance to ensure continued compliance with their obligation to protect systems and facilities used to access the PEXA system, and have been reminded of the importance to:

- Maintain updated anti-virus software, operating systems and internet browsers - Access secure Wi-Fi (i.e. not public)
- Use a Virtual Private Network (VPN) to maintain a secure connection with their corporate services and applications
- Implement Multi-factor Authentication (MFA)
- Protect and optimise passwords
- Remain vigilant to scams (e.g. email phishing)

We have also provided relevant communications to peak industry bodies for broader distribution to their members and we have shared with our members relevant notifications and guidance from ARNECC, land registries and peak industry bodies. We also continue to provide member support services by telephone, email and virtual appointment where guidance for managing cyber security risks is reiterated.

Unsupported Software

Some of our members connect to PEXA using computer systems with outdated software that is not sustained by continued updates and upgrades. Such systems contain weaknesses which may be exploited, thereby making them particularly vulnerable to targeted cyber attack. With the rapid shift to remote working, PEXA has detected an increase in the use of unsupported software, presumably due to an uptake in the use of personal computers which may be less modern.

This represents a development of a known issue that PEXA has been working to resolve through the identification and recording of users accessing PEXA on unsupported operating systems or browsers. We recognise the importance of members' needs to continue transacting property during these unprecedented circumstances, and we have therefore expanded our access monitoring and continue to provide guidance to support members with upgrading their software to safeguard against cyber crime.

In the context of the ongoing COVID-19 pandemic and the likelihood that working from home and otherwise working outside of the traditional office setting will continue, we consider it essential that practitioners develop and maintain a high level of knowledge and awareness of effective cyber security practices and strategies.

We hope that these comments are useful to you in the course of the VLSB+C's Review into CPD for practitioners, and we would be happy to discuss any of these details with you as the Review progresses.

Kind regards

Amy Gerraty
General Manager, Regulatory and Government Affairs
+61 (0) 409 360 710