Canadian Association of Private Lenders

Via email: samanthagale098@gmail.com

April 29, 2022

Financial Services Regulatory Authority of Ontario (FSRA)
The Mortgage Broker Regulators' Council of Canada (MBRCC)
25 Sheppard Avenue West, Suite 100
Toronto, ON
M2N 6S6
Submitted electronically via feedback form

Re: Feedback on Proposed Cybersecurity Reporting Protocols and MBRCC Standards on Cybersecurity

We write on behalf of the newly formed Canadian Association of Private Lenders, which represents the interests of private mortgage lenders, investors and administrators across Canada. One of the rationales for establishing this association is to focus private lending dialogue on regulatory reform.

More specifically, we are writing to provide comments on the Financial Services Regulatory Authority of Ontario's (FSRA's) proposed guidance No. MB0048INF which sets out two proposals. One is for FSRA to adopt the MBRCC cybersecurity guidance for the mortgage broker industry, and the second is to establish reporting protocols for registrants which have been exposed to a cybersecurity incident which could materially impact client privacy and information. In addition, we intend to provide feedback directly to the MBRCC on its cybersecurity guidance.

We observe that the media has reported on a significant number of cybersecurity threats occurring over the pandemic period, when many employees started to work remotely and businesses began relying more than ever on electronic systems to collect and process data. Regulators in other financial services sectors and jurisdictions, such as the securities and financial institutions sectors in the US and Canada, appear to have responded by implementing cybersecurity guidance and incidence reporting requirements. The cybersecurity proposals of the MBRCC and FSRA appear to be aligned with these other initiatives. We support strengthened cybersecurity measures for the mortgage industry which aim to protect client information in a rapidly evolving digital business ecosystem. However, we wish to make the following additional comments concerning the proposals.

Definition of Regulated Entity and Information Asymmetry

The last sentence of section 2 of the MBRCC guidance explains that " Regulated entities are third-party service providers to financial institutions. Regulated entities should ensure that they understand and are compliant with a financial institution's expectations of third-party service providers regarding cybersecurity and, more broadly, information security." This description of entities regulated under the various provincial mortgage licensing statutes is incorrect. Many licensees are not third-party service providers to financial institutions. These licensees include private mortgage lenders, brokerages which deal with private mortgage lenders and investors, and mortgage administrators. For those licensees who do arrange mortgages for financial institutions, we note that there is a considerable challenge with information asymmetry between banks and brokerages. While financial institutions may choose to publish or otherwise convey their cybersecurity protocol expectations to third parties, brokerages simply do not have the power to compel financial institutions to provide this information. In our view there is an inherent lack of fairness in imposing a regulatory expectation on licensees when the licensees may lack the power, through no fault of their own, to comply with the regulatory expectation.

Third Parties - Verification of Cybersecurity Practices

Section 4 of the MBRCC guidance states "Regulated entities are responsible for protecting their clients' information against cyber incidents by ensuring that their third-party service providers have cybersecurity preparedness practices in place." However, many regulated entities are significantly smaller enterprises than the third-party service providers which assist with the mortgage arranging process, and as such, the regulated entities may not possess the requisite power to compel service providers to disclose their cybersecurity practices. Take for example, the multi-national credit reporting agency Equifax, which carefully vets mortgage entities prior to accepting account applications from them – while we might assume that such a large, well-established entity engages in the highest level of cybersecurity preparedness, it would be surprising if, during the account vetting process, Equifax was open to discussing their own cybersecurity practices for the purpose of them being accepted by the prospective account holder. As stated above, there is an inherent lack of fairness in imposing a regulatory expectation on licensees when the licensees may lack the power, through no fault of their own, to comply with regulatory expectation.

Statutory Authority and Regulatory Creep

The MBRCC's cybersecurity guidance appears to be formulated using principles-based standards, which we consider to be appropriate and is in alignment with how cybersecurity standards are imposed in other regulated financial services sectors. However, we do note that the mortgage brokering sector in Canada is currently regulated using primarily rules based and not a principles-based oversight. One challenge with creating guidance that is not directly linked to an overarching licensing

statute, is that it is likely to cause confusion to industry members, as there is uncertainty as to what regulatory standards are subject to regulatory proceedings for non-compliance. The MBRCC guidance advises that no new obligations are created: "MBRCC considers this guidance to be aligned with, and therefore can be interpreted in a manner consistent with, all existing requirements, rules, and standards of conduct." The regulatory authority to enforce privacy standards, as is noted in the FSRA discussion of its consultation, exists with privacy regulators under a variety of federal and provincial privacy statutes. Anticipated changes to privacy legislation in the future are significant, and include heavier duty standards, reporting requirements and significantly higher penalties.

However, matters are confused when FSRA's separate guidance on the subject contained in its consultation is that "Mortgage brokerages and administrators should notify FSRA if they experience a cybersecurity incident that could have a material impact on client information …". This does appear to create a new obligation, contrary to other statements contained in the guidance. We further note that section 48(2) of MBLAA makes it an offence for persons who fail to comply with standards that are applicable to their license. From a technical perspective, the MBRCC cybersecurity guidance does not appear to qualify as a "standard", although the wording of section 48(2) might make it appear to. The transition to principles-based rules on subject matters which are directly regulated by another regulator in conjunction with new incidence reporting requirements to FSRA potentially creates blurred lines leading to confusion over regulatory oversight and obligations.

We support the MBRCC's and FSRA's focus on strengthening the protection of consumer information from cyber-attacks. However, regulators may wish to consider the comments noted above in finalizing the guidance. Thank you for the opportunity to provide comments on this subject. Please know that we are available to discuss these issues more fully if you wish.

Yours truly,

Samantha Gale