ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Box 348, Commerce Court West
199 Bay Street, 30th Floor
Toronto, Ontario, Canada M5L 1G2
www.cba.ca

Neil Parmenter
President and CEO
Tel: (416) 362-6093 Ext. 211
nparmenter@cba.ca

November 9, 2017

Mr. Dan Ruimy, M.P.
Chair, Standing Committee on Industry, Science and Technology
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6
Canada

Dear Mr. Ruimy:

The Canadian Bankers Association (CBA) welcomes the opportunity to provide the banking industry's perspective on Canada's Anti-Spam Law (CASL) in the context of the statutory review being undertaken by the House of Commons Standing Committee on Industry, Science, and Technology (Committee).

The CBA is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals.

The Canadian banking industry fully supports the policy goal of reducing malware and spam. We have serious concerns, however, that CASL contains several provisions that are overly broad and unclear, making compliance with the legislation exceptionally challenging. In addition, several provisions complicate and impede common business practice and innovation without supporting the policy goal. Further, the consequences of an inadvertent or technical breach of the law are overly severe. If these issues remain unaddressed, CASL will stifle business innovation and growth in Canada, particularly in the development of e-commerce and the digital economy.

While the CBA has many technical recommendations on how CASL should be improved, this letter addresses the most important overarching elements. We would welcome the opportunity to further engage with the Committee as it completes its statutory review of the legislation.

Definition of a Commercial Electronic Message

It is difficult for well-intentioned businesses to comply with CASL because of a lack of clarity in many of the provisions. Most notably, the definition of a "commercial electronic message" (CEM) is overly broad and includes many types of service messages that most Canadians would not view as spam. As currently drafted, even if the primary purpose of a message is not related to promotion of a commercial activity, the message could be subject to CASL requirements, and therefore subject to penalties for technical non-compliance.

The legislation must be amended to ensure that the definition of CEM is limited to a message whose primary purpose is to encourage participation in a commercial activity. This would help ensure that CASL does not inadvertently cover messages that are not commercial advertisements or do not promote a commercial product or service. Such an amendment would improve CASL without undermining its primary purpose of reducing malware and spam.

Transactional, Relationship and Service Messages

CASL deems transactional and relationship messages to be a special category of CEMs. Transactional and relationship messages can be sent without consent, but must comply with the form requirements, i.e., sender identification and unsubscribe requirements. However, these messages are specifically exempt from the definition of CEM in other countries, specifically U.S. and New Zealand.

The scope of CASL also needs to be narrowed, particularly in terms of transactional messages (s.6(6)) that provide important details about the status of a transaction, or factual information regarding the ongoing use of a product or service. For example, based on the current drafting, a message signifying that a transaction is final or has been completed, or that a credit card is ready for use, could be deemed to be a CEM and subject to compliance with CASL. These types of transactional or service messages are integral to communicating important information to consumers about their existing products and services, and should be exempt from CASL.

Implied Consent, Business to Business Exemption, and Record Keeping Requirements

Meaningful business innovation often calls for the expansion of existing relationships or the development of new relationships. These business imperatives have not been adequately integrated into CASL. CASL's concept of implied consent, and the rules associated with the expiry of such consent, are overly complex and create onerous record keeping requirements associated with tracking and proving consent. To facilitate innovation, CASL's concept of implied consent must be amended to allow businesses more flexibility to send CEMs. Canadian businesses, just like their counterparts in other jurisdictions such as Australia and New Zealand, should be allowed to send messages where consent can be reasonably inferred from: (i) the conduct; and (ii) the business and other relationships of the individual or organization concerned.

The business to business exemption in section 3(a)(ii) of the Electronic Commerce Protection Regulations does not address the challenges of communication between businesses in the modern digital world. This exemption was introduced in response to business concerns about CASL impairing standard business to business communication. In order to benefit from the

exemption, there must be a relationship between the business sending the message and the business receiving the message. In reality, it appears to be difficult to establish proof of a relationship. In fact, prior transactions and prior communications between the businesses does not appear to provide evidence of a relationship. Clarifying the business to business exemption would provide much needed assistance to Canadian businesses.

Finally, the record keeping requirements promulgated by the Canadian Radio-television and Telecommunications Commission must also be revisited to alleviate the administrative burdens associated with proving implied consent. Maintaining a record of all evidence of implied consent is costly and very difficult to operationalize.

Enforcement

Failure to comply with CASL carries a potential administrative monetary penalty (AMP) of up to $1 million for individuals and up to $10 million for businesses. Penalties may be charged per violation and violations may be separately assessed for each day of non-compliance, even in cases of inadvertent non-compliance. These AMPs are much higher than fines in other jurisdictions; for instance, the US' CAN-SPAM Act provides that each email is subject to penalties of up to approximately $40,000. We are not opposed to enforcement and AMPs, however, we believe these penalties must be commensurate with the potential level of harm that could arise from a breach of CASL.

Private Right of Action

The CBA was pleased by the government's decision earlier this year to delay the private right of action (PRA), and we strongly support removal of the PRA provisions from CASL. We have joined many other stakeholders in expressing concerns that the PRA creates extensive class action risk, even in cases of technical non-compliance by businesses with an otherwise excellent record of compliance. The PRA provisions will make frivolous class actions easier and could result in serious reputational damage for businesses in Canada. It is also worth noting that collecting on a judgement against a business based outside Canada, where much of the spam targeted at Canadians originates, would be very difficult.

If the government's decision following this statutory review is to implement the PRA, it must only occur after CASL is amended to ensure that the PRA cannot be used to penalize a legitimate business, which has conducted due diligence, for technical or inadvertent violations of CASL requirements that cause no harm to recipients. In addition, the scope of the PRA must be narrowed. As currently drafted, litigants do not have to prove actual damages to bring an action and it is open to individuals, not just Internet Service Providers (ISPs). This is inconsistent with other comparable international legislation, such as the US' CAN-SPAM Act. We suggest restricting the PRA along the lines of what has been done in the US, so that only ISPs can file a class action. Additionally, it should only apply to egregious behaviours where actual damage has been done and if it was conducted by a person who acted knowingly or recklessly. Finally, the legislation should be amended to clarify that no PRA may be brought for events that occurred prior to its implementation date.

Conclusion

In its current form, CASL, and the class action risk presented by the PRA, will act as a disincentive for businesses to operate and innovate in Canada, undermining our place in the global digital economy. As more and more consumers shift to digital interactions, businesses must be able to communicate with their clients under legislation that is clear, while meeting the objective of reducing the amount of malware and spam Canadians receive.

As the financial sector undergoes tremendous change driven by consumers' use of technology, banks and new entrants are delivering more financial services digitally. Canadians have come to expect greater convenience when using and accessing financial services, with nearly three-quarters of Canadians primarily doing their banking online or on their mobile device. We fully expect this trend will continue. It is critical that the Canadian banking sector be able to communicate with their clients under a legislative framework that encourages innovation.

We encourage the Committee to consider our comments when developing its recommendations to the government. We look forward to working with the Committee as it completes its statutory review of CASL. Should you have any questions, please do not hesitate to contact me directly or Tim Downing, Director of Legislative Affairs, at 613-234-4431 ext. 623 or tdowning@cba.ca.

Sincerely,