30 Eglinton Avenue West, Suite 740
Mississauga ON L5R 3E7
Tel: (905) 279-2727
Website: www.ifbc.ca

May 31, 2016

Data Breach Consultations
Privacy and Data Protection Policy Directorate
Innovation, Science and Economic Development Canada
235 Queen Street
Ottawa ON K1A 0H5

Sent by Email: ic.ised.breach-atteinte.isde.ic@canada.ca

Dear Sir/Madam:

Subject: Data Breach Notification and Reporting Regulations

Independent Financial Brokers of Canada (IFB) appreciates the opportunity to provide input on this discussion paper. We only recently became aware of this consultation, however, we wanted to briefly comment on some of the issues under consideration. We will look forward to participating in the future as more detailed regulations are released for public input.

IFB is a voluntary, professional association with approximately 4,000 members across Canada. Our members are licensed financial advisors who provide tailored financial advice and investment solutions to consumers every day. A distinguishing feature of this association is that IFB only represents independent advisors, meaning those who have the ability to offer clients products from a variety of companies. IFB does not represent career agents or employees of financial firms.

IFB members are generally licensed to sell life/health insurance and/or mutual funds, although many hold complementary financial licenses or professional accreditations which allow them to serve their clients in a more holistic way. Most are self-employed and operate small to medium-sized businesses in their local community.

With this context in mind, our comments focus on the potential effect of these amendments on our members (as small business people), their clients (who are generally individuals and families), and on IFB as a corporate entity.

IFB is a federally incorporated not-for-profit corporation and is subject to PIPEDA. Members who reside in BC and Alberta are outside of PIPEDA and subject to their provincial PIPA Acts.

IFB supports the risk-based approach underlying this legislation. Small and medium sized businesses face significant regulatory burden and costs, and these are often disproportionately high when compared to the cost of compliance for larger businesses.

Breach notification threshold

In general, IFB supports a mandatory breach notification requirement. However, not all breaches pose a "real risk of significant harm", and organizations should have flexibility in determining whether notification should occur, and how it should be done. Establishing a harm threshold helps to address the potential for over-reporting by organizations. Such reporting can create undue concern for consumers when the risk of misuse of their information is minimal. Establishing a harm threshold does not preclude voluntary disclosure by organizations, a practice which is not unusual and often considered a best practice.

Where possible, we prefer a harmonized approach with similar legislation, like that in Alberta and BC. As noted, many IFB members are licensed to conduct business in multiple jurisdictions and differences in reporting requirements can create confusion and hinder compliance.

Report to Commissioner

IFB prefers a requirement to report a breach to the Privacy Commissioner as soon as possible, rather than specifying a formal timeline. When a breach occurs, organizations need time to investigate the circumstances, and the potential impact. As the investigation proceeds, the details and severity of the breach may change.

We agree that the Commissioner should be informed when the information provided in the original breach notification is substantially different than first reported, and that any reporting should utilize a secure format.

Recordkeeping

The recordkeeping provisions, as currently drafted, are a concern to us. Specifically, the requirement to maintain records of any data breach, regardless of its risk of significant harm, seems unduly onerous. We prefer an approach where the recordkeeping requirement is aligned with the reporting requirement, so that only those incidents where some material harm has been assessed, will invoke the need to retain records.

We concur that a report, when made to the Privacy Commissioner, would satisfy the record-keeping requirement. This would help to reduce the burden on organizations and duplication of such records. The obligation to maintain a data breach record should apply only to breaches the organization has actual knowledge of, and not assumed breaches.

Penalties

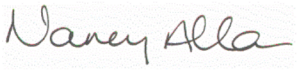
Under the Act, knowingly violating the breach notification or record keeping requirements (including failing to keep records) may result in: i) a summary conviction and a $10,000 fine, or ii) an indictable offence and a fine not exceeding $100,000 per occurrence. These penalties are significant and under the current provisions, could be triggered in the event that a breach - even where the risk to an individual is minimal - is not reported to the Commissioner, or a record kept. Clearly the impact of such

a penalty, for a financial advisor operating a small business would be devastating, with no corresponding harm to consumers. In our view, "harm" should be the test for reporting.

This concludes our remarks. IFB looks forward to commenting further as this consultation process progresses.

Please contact the undersigned, or Susan Allemang, Director, Policy & Regulatory Affairs (email: sallemang@ifbc.ca) should you wish to discuss or have questions.

Yours truly,



Nancy Allan
Executive Director
Email: allan@ifbc.ca