Blaney McMurtry LLP

PUBLICATION

CRTC Issues Updated Guidance on Canada's Anti-Spam Legislation

Date: July 07, 2014

Original Newsletter(s) this article was published in: International Business Bulletin: June 2014

Introduction

We previously provided a detailed analysis of Canada's Anti-Spam Legislation[1] ("CASL"). The provisions that regulate the transmission of commercial electronic messages ("CEMs") came into force on July 1, 2014, and are now effective.

The Canadian Radio-television and Telecommunications Commission ("CRTC") has recently revised its Frequently Asked Questions Page (the "Revised FAQ") to provide additional guidance on CASL. It has also issued Compliance and Enforcement Bulletin #2014-326 (the "Bulletin"), which provides guidance on the development of corporate compliance programs.

Key issues addressed in this recent guidance are discussed in greater detail below.

Transitional Provisions

According to Section 66 of CASL, a person's consent to receive CEMs from another person is implied for a period of three years beginning July 1, 2014, or until the person withdraws his or her consent, provided that:

a. Those persons have an existing business or non-business relationships, as those terms are defined in CASL; and

b. The relationship includes the communication of CEMs between them.

Although Section 10 of CASL already provides for implied consent, during the transitional period, the definitions of "existing business relationship" and "existing non-business relationship" will not be subject to the two-year/six month limitation periods that would normally apply. This is intended to provide additional time for businesses and individuals to seek express consent.

The Revised FAQ clarifies that one-way communication of CEMs (i.e. where a business sends CEMs to a consumer with whom it has an existing relationship) will be acceptable for the purpose of Subsection 66(b). It does not need to be two-way communication.

The Revised FAQ also clarifies that express consent does not expire after a certain period of time has elapsed. If valid express consent is obtained before July 1, 2014, this express consent remains valid after CASL comes into force; it does not expire until the recipient withdraws their consent.

In addition, the Revised FAQ clarifies that the existing business relationship or existing non-business relationship must be created prior to July 1, 2014, in order for the three-year transitional provision to apply. Any existing business relationship or existing non-business relationship created after July 1, 2014, will be subject to the limitation periods described in Section 10.

Social Media

Section 6 exempts certain CEMs, including a CEM sent to an individual with whom the sender has a personal relationship. The Revised FAQ clarifies that a "personal relationship" requires that the real identity of the individual who alleges a personal relationship be known by the other individual involved in such a relationship (as opposed to instances where a virtual identity or an alias is used).

It further states that using social media or sharing the same network does not necessarily reveal a personal relationship between individuals. The mere use of buttons available on social media websites - such as clicking "like," voting for or against a link or post, accepting someone as a "friend," or clicking "follow" - will generally be insufficient to constitute a personal relationship.

Corporate Compliance Programs

OVERVIEW

The stated purpose of the Bulletin is to provide general guidance and best practices for businesses on the development of corporate compliance programs. CRTC staff may take into consideration the existence and implementation of an effective corporate compliance program, if the business presents the program as part of a due diligence defence in response to an alleged violation of CASL. CRTC staff can also take the existence of such a program into consideration when determining whether a violation of CASL is an isolated incident or is systemic in nature, and whether sanctions against a business should include administrative monetary penalties.

According to the Bulletin, an effective corporate compliance program should address the following elements: (a) senior management involvement; (b) risk assessment; (c) written corporate compliance policy; (d) record keeping; (e) training; (f) auditing/monitoring; (g) complaint-handling system, and (h) corrective (disciplinary) action. The Bulletin provides guidance on each of these elements.

SENIOR MANAGEMENT INVOLVEMENT

In the case of large businesses, the business's senior management should consider playing an active and visible role in fostering a culture of compliance within their organization. In addition, a member of senior management could be named as the business' chief compliance officer, who is responsible and accountable for the development, management, and execution of the business' corporate compliance program. In the case of small and medium-sized businesses, the business could identify a point person who is responsible and accountable for compliance with CASL.

RISK ASSESSMENT

The chief compliance officer or point person should consider conducting a risk assessment to determine which business activities are at risk for the commission of violations under CASL. The chief compliance officer or point person should then develop and apply policies and procedures to mitigate those risks.

WRITTEN CORPORATE COMPLIANCE POLICY

After conducting a risk assessment, the chief compliance officer or point person should consider developing a written corporate compliance policy. The business should make this policy easily accessible to all employees, including managers. The business could update the policy as often as necessary to keep pace with changes in legislation, non-compliance issues, or new services or products. The policy may also:

a. Establish internal procedures for compliance with CASL;

b. Address related training that covers the policy and internal procedures;

c. Establish auditing and monitoring mechanisms for the corporate compliance program;

d. Establish procedures for dealing with third parties (for example, partners and subcontractors) to ensure that they comply with CASL;

e. Address record keeping, especially with respect to consent; and

f. Contain a mechanism that enables employees to provide feedback to the chief compliance officer or point person.

RECORD KEEPING

Businesses should consider maintaining hard copy and/or electronic records of the following:

a. The business' CEM policies and procedures;

b. All unsubscribe requests and actions;

c. All evidence of express consent (i.e. audio recordings or forms) by consumers who agree to be contacted via CEM;

d. CEM recipient consent logs;

e. CEM scripts;

f. Actioning unsubscribe requests for CEMs;

g. Campaign records;

h. Staff training documents;

i. Other business procedures; and

j. Official financial records.

TRAINING PROGRAM

The chief compliance officer or point person should consider developing and implementing a training program, including refresher training, regarding the corporate compliance policy for current and new employees, including managers. After training, employees could provide a written acknowledgment confirming that they understand the corporate compliance policy, and these written acknowledgments should be recorded and maintained.

The business could also monitor employee comprehension of the corporate compliance policy, and the training program could be adapted and re-administered accordingly. The business could re-administer training following important modifications or updates to the corporate compliance policy. The chief compliance officer or point person could also evaluate the effectiveness of this training at regular intervals. The chief compliance officer or point person should also consider monitoring any legislative or regulatory changes, and modifying or updating the corporate compliance policy and the related training accordingly.

When assessing what to include in the training program, businesses should consider the following:

a. Providing an understanding of what is required under CASL and the penalties for not meeting those requirements;

b. Policies and procedures associated with the business; and

c. Background information on CASL.

AUDITING AND MONITORING

The chief compliance officer or point person could be responsible for ensuring that audits are conducted at regular intervals with or without external help. Auditing may involve developing

and implementing a quality assurance program that would, for example, monitor a statistically significant percentage of the business' email marketing campaigns. The results of all audits should be recorded, maintained, and communicated to senior management. Following an audit, the business should address any recommendations and modify or update the corporate compliance policy as appropriate.

COMPLAINT-HANDLING SYSTEM

The chief compliance officer or point person could put in place a complaint-handling system to enable customers to submit complaints to the business. The business should respond to and resolve complaints within a reasonable or predetermined period of time.

CORRECTIVE (DISCIPLINARY) ACTION

Businesses could have an organizational disciplinary code to address contraventions. This code would help to: (a) demonstrate a business' credibility regarding its corporate compliance policy, and (b) deter possible employee contraventions of the corporate compliance policy.

Businesses should consider taking corrective or disciplinary action, or providing refresher training, as appropriate, to address contraventions of the corporate compliance policy. Businesses could maintain a record of the contravention and the action taken in response to the contravention.

---

[1] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23).*