



A Million Reasons to Comply -- CRTC Issues \$1.1 Million Penalty Against Training Firm For Anti-Spam Law Violations

by Dina L. Maxwell

Originally published in *Blanelys on Business* (June 2015)



Dina L. Maxwell is a member of Blaney McMurtry's Insurance Litigation and Privacy Groups. Her practice includes insurance defence, with a focus on professional negligence, privacy law and investigations, and insurance coverage. Called to the Ontario Bar in 2010, Dina holds a J.D. from the University of Toronto and a B.A. from Harvard. A member of the International Association of Privacy Professionals and a certified Information Privacy Professional (CIPP) in Canada and the United States, Dina has appeared as counsel on applications, motions and interlocutory proceedings before the Ontario Superior Court of Justice.

Dina may be reached directly at 416.593.3949 or dmaxwell@blaney.com.

The Canadian Radio-television and Telecommunications Commission (CRTC) has issued its largest fine ever as a result of violations under Canada's Anti-Spam Legislation (CASL).

The action sends a powerful message to businesses that market directly by electronic means, such as text messages and email, and makes clear the need to have in place a compliance regime to protect against CASL complaints.

CRTC Issues Notice of Violation Against Compu-Finder

The fine in question is contained in a Notice of Violation issued by the CRTC on March 5, 2015 against Compu-Finder, a Quebec based company, which was cited for multiple CASL violations. Compu-Finder is in the business of advertising training courses to businesses on topics such as management, social media and professional development.

During the course of the CRTC's investigation, it determined that Compu-Finder sent commercial electronic messages (CEMs) without the recipient's consent and that the CEMs did not contain functioning unsubscribe mechanisms. The violations allegedly occurred between July 2, 2014 and September 16, 2014. The CRTC also noted that complaints against Compu-Finder accounted for 26 per cent of all complaints submitted within Compu-Finder's industry sector.

Compu-Finder had 30 days to either pay the penalty or submit written representations to the CRTC challenging the CRTC's decision. Compu-Finder also had the scope to provide the CRTC with an undertaking to take certain measures to comply with CASL. (The CRTC has the discretion to accept and consider such an undertaking before disposing of the matter.) The CRTC said at the end of May that the case was "still ongoing."

Overview of CASL

CASL came into force on July 1, 2014. It applies to all forms of electronic communication (including emails, text messages, and instant messages) that promote or encourage commercial activity.

CASL contains three key criteria that businesses must follow when sending CEMs.

First, businesses must have the recipient's consent before sending CEMs. This consent must be explicit or obtained on an opt-in, rather than opt-out, basis. Consent can be implied in certain situations, such as when the parties have a pre-existing business relationship.

Second, CEMs must contain information identifying the name of the sender and its contact information (email, address, telephone number, website, etc.).

Third, the CEM must contain a mechanism through which the recipient can, at no cost, 'unsubscribe' from receiving future communications from the sender. Businesses have 10 business days in which to remove the recipient from its lists.

Penalties Under CASL

As demonstrated by the Compu-Finder case, penalties for CASL violations can be steep. The maximum penalty for a violation is \$1 million in the case of an individual and \$10 million per violation in the case of any other "person" (e.g. for-profit and not-for-profit corporations, partnerships, joint ventures etc.). When issuing a penalty, the CRTC will consider various factors outlined in section 20 of CASL. Such factors include, but are not limited to, the purpose of the penalty, the nature and scope of the violation, the sender's history with respect to any previous CASL violation, any financial benefit that the sender obtained from the CASL violation, the sender's ability to pay the penalty, and whether the sender has voluntarily paid compensation to a recipient affected by the violation.

If the CRTC determines that CASL has been violated, it may opt to take measures other than issuing monetary penalties. For example, it may discuss corrective actions with the sender, which may lead to an undertaking or other corrective measures. The CRTC can also issue warning letters, preservation demands (requiring that various documents be retained), notices to produce (records of various kinds), restraining orders and notices of violation.

Compu-Finder is only one example of recent penalties issued under CASL. On March 25, 2015, Plentyoffish Media Inc., which operates the online dating service Plenty of Fish, paid \$48,000 as part of an undertaking for violating CASL. After receiving complaints from members of the public, the CRTC launched an investigation and determined that Plenty of Fish had allegedly sent CEMs to registered users of its online dating service which contained an unsubscribe mechanism that was not clearly and prominently set out, and which could not be readily performed, as required by CASL. As part of the undertaking, Plenty of Fish will develop and implement a CASL compliance program that will include training and education for staff and the development of corporate policies and procedures.

Best Practices for Businesses to Avoid CASL Complaints

As of January 6, 2015, more than 210,000 complaints of alleged violations of CASL had been made to the CRTC. The CRTC has confirmed that it will focus on the most severe types of violations when launching investigations. Nevertheless, these recent cases underscore the importance of understanding CASL and ensuring that your company's CEM-sending practices comply with the law. Businesses are encouraged to adopt CASL-compliant processes such as:

- developing a policy and guidelines for determining whether a message is actually a CEM and whether an exception applies;
- determining if electronic addresses your organization collected previously can still be used under the existing law and, if not, either scrub existing databases or obtain express consent;
- ensuring all CEM templates contain all mandatory identity and contact information as well as a compliant unsubscribe mechanism; and
- auditing compliance with CASL and revise as necessary.

Conclusion

CASL has been in force for less than a year. It is evident that the CRTC is taking complaints seriously and will issue penalties where appropriate.

In addition to the threat of investigations, penalties, and potential damage to one's reputation, businesses should also be aware that CASL's provisions for private rights of action will come into force in July 2017, which will allow private citizens to sue CASL violators in civil actions.

Businesses are strongly encouraged to be proactive with respect to compliance in order to avoid becoming the targets of CASL complaints. ■