CASL Bulletin

December 2019

CASL Enforcement Action – $115,000 in Penalties for Distributing Malware

On December 10, 2019, the Canadian Radio-television and Telecommunications Commission issued a notice of violation under *Canada's Anti-Spam Legislation* (commonly known as "CASL") against two individuals operating Orcus Technologies for allegedly aiding the installation and operation of malware known as "Orcus RAT". The notice imposes $115,000 in penalties.

CASL

CASL creates a comprehensive regime of offences, enforcement mechanisms and potentially severe penalties designed to prohibit the sending of unsolicited or misleading commercial electronic messages ("CEMs"), the unauthorized commercial installation and use of computer programs on another person's computer system and other forms of online fraud.

For most organizations, the key parts of CASL are the rules for CEMs. Subject to limited exceptions, CASL creates an opt-in regime that prohibits the sending of a CEM unless the recipient has given consent (express or implied in limited circumstances) to receive the CEM and the CEM complies with prescribed formalities (e.g. information about the sender and an effective and promptly implemented unsubscribe mechanism) and is not misleading. See BLG bulletin *Canada's New Anti-Spam and Online Fraud Act – Some Frequently Asked Questions*.

CASL also prohibits, subject to limited exceptions, the installation and use of a computer program on another person's computer system, in the course of a commercial activity, without the express consent of the owner or authorized user of the computer system. The computer program rules apply to almost any computer program (not just malware, spyware or other harmful programs) installed on almost any computing device (including mobile phones) as part of a commercial activity (regardless of expectation of profit). See BLG bulletins *CASL – Rules for the Installation and Use of Computer Programs* and *CASL – Regulatory Guidance for Computer Program Installation Rules*.

CASL imposes liability not only on an organization that directly violates CASL (e.g. by sending a prohibited CEM or installing a prohibited computer program) but also on an organization that causes or permits a CASL violation, or who aids, induces or procures a CASL violation. CASL

also provides that an organization is vicariously liable for CASL violations by its employees and agents (e.g. digital marketing service providers) within the scope of their employment or authority, and corporate directors and officers are personally liable if they direct, authorize or assent to, or acquiesce or participate in, a CASL violation. Organizations, directors and officers might avoid liability if they establish that they exercised due diligence to prevent the CASL violation.

CASL violations can result in potentially severe administrative monetary penalties – up to $10 million per violation for an organization and $1 million per violation for an individual – in regulatory enforcement proceedings. CASL includes a private right of action that is not in force. See BLG bulletin *CASL – Government Suspends Private Right of Action*.

The Canadian Radio-television and Telecommunications Commission ("CRTC") is responsible for enforcing CASL's rules regarding CEMs and computer program installation, and has various enforcement tools for that purpose. Since CASL came into force in 2014, CRTC has taken enforcement action against organizations and individuals who have violated CASL, and has issued enforcement decisions and accepted voluntary undertakings (settlements). See BLG bulletins *CASL – Year in Review 2018*, *CASL – Year in Review 2017*, *CASL – Year in Review 2016* and *CASL – Year in Review 2015*.

In December 2017, the House of Commons Standing Committee on Industry, Science and Technology issued a report titled *Canada's Anti-Spam Legislation: Clarifications are in Order*, which recommends some changes to CASL. In April 2018, the government released an official response to the report. See BLG bulletin *New Committee Report on CASL Highlights Need for Clarification and Education*.

CASL Enforcement Action – Orcus RAT

On December 10, 2019, the CRTC announced the issuance of a notice of violation against two individuals operating a partnership known as Orcus Technologies, alleging that they violated CASL's computer program rules by developing, selling and promoting malware known as "Orcus RAT", which enables hackers to install the program and take control of a victim's computer without their knowledge or consent.

The CRTC's investigation of Orcus Technologies commenced in February 2018 and involved an international coordinated effort with the Royal Canadian Mounted Police (RCMP), the U.S. Federal Bureau of Investigation and the Australian Federal Police. The investigation involved the CRTC's collection of documents from third party industry participants (e.g. cybersecurity firms, internet service providers and web hosts) pursuant to CASL's information gathering provisions, and the execution of warrants under CASL and the *Criminal Code* by the CRTC and the RCMP.

The CRTC's announcement and notice of violation explain as follows:

- Orcus Technologies is a partnership operated by Vincent Griebel (a German national) and John Paul Revesz (an Ontario resident).
- Orcus Technologies developed, distributed, promoted, sold and supported a remote administration tool under the name "Orcus RAT". Orcus RAT is not a typical administration tool, but rather is a remote access trojan – a particularly dangerous type of malware that allows a hacker to install and take full administrative control of another person's computer system through a remote network connection without their knowledge or consent. Unlike lawful remote administration tools, remote access trojans are designed for stealth installation and operation and for the infliction of harm.
- Griebel and Revesz promoted the malicious features of Orcus RAT.
- Orcus RAT has been sold at least 1,300 times. While the total number of computer systems infected with Orcus RAT is unknown, it is expected to be "considerable".
- A Canadian virtual private server was used by an Australian hacker to install Orcus RAT on hundreds of computer systems worldwide, including 23 computer systems located in Canada.
- From 2016 to 2019, Revesz operated a dynamic domain name server service that was used by hackers to install different kinds of remote access trojans on computer systems and to communicate with the infected computer systems in Canada and abroad.

The CRTC notice of violation alleges that Griebel and Revesz contravened CASL by aiding malicious actors to install the Orcus RAT without consent, in the course of commercial activity, on computer systems located in Canada. The notice also alleges that Revesz contravened CASL by selling a dynamic domain name server service used by hackers to communicate with remote access trojans on computer systems in Canada and abroad. The notice imposes a total administrative monetary penalty of $115,000 on Griebel and Revesz. Griebel and Revesz have 30 days to file representations against the notice of violation or pay the penalty.

Comment

CRTC's enforcement action against the principles of Orcus Technologies illustrates how CASL imposes liability on individuals who aid other persons to commit a CASL violation. CRTC has encouraged organizations to develop and implement a credible and effective CASL compliance program as a risk management strategy to reduce the likelihood of CASL contraventions and to help establish a due diligence defense and ameliorate potential sanctions if a CASL contravention occurs. For more information, see BLG bulletin *CASL Compliance Programs — Preparing for Litigation*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's national CASL Group includes lawyers, located in BLG's offices across Canada, with expertise in CASL, privacy law, cyber risk management and class action litigation. We provide both proactive CASL compliance advice and legal advice to help respond to a CASL contravention. Additional information about BLG's national CASL Group and our services is available at **blg.com/CASL**.