

February 6, 2018

Canada Requires VoIP Service Providers to Implement Technical Measures to Combat Robocalls—A Likely Preview of U.S. Regulation

Everyone hates random telemarketing robocalls. Many of these calls originate overseas and are sent by those with no regard for rules designed to avoid such calls, like the Do Not Call Registry. New technologies make it easier and cheaper to blast out these calls and Voice over Internet Protocol (VoIP) services make it easy to disguise the true origin of the calls. Unscrupulous telemarketers can insert a false phone number so that the number that shows up on caller ID looks like a local number, or, worse, the number of an agency like the IRS. This is called spoofing. Spoofing can lead to more than annoyance, it can enable scamming and fraud.

The Federal Communications Commission (FCC) has taken a number of steps to begin addressing the problem. In November, for example, the FCC issued an [order](#) authorizing telephone companies to begin blocking calls from certain types of numbers that cannot or should not be used to make calls. To address the problem of spoofing more specifically, the FCC issued a [Notice of Inquiry](#), an initial rulemaking step, to potentially establish a new caller authentication technology called SHAKEN/STIR that would be used by the telephone companies. Under this technology, a system would be established to verify that the phone number really belongs to the person making the call.

The Canadian regulatory authorities have [moved ahead](#), requiring Canadian VoIP providers to implement SHAKEN/STIR in a little over a year, by March 31, 2019, and it is taking concrete steps to implement a process to identify the originator of unlawful robocalls. These steps likely preview the approach the FCC may follow in the coming months as it moves through the rulemaking process, so it is worth a look at the actions taken by the Canadian Radio-television and Telecommunications Commission (CRTC).

Disregarding numerous comments by Canadian telecommunications providers that it would be premature to adopt SHAKEN/STIR because standards are still under development, the CRTC nevertheless ordered its implementation. It noted that SHAKEN/STIR was the “only current viable solution that can provide consumers with a measure of additional trust in caller ID.” It expects the standards for SHAKEN/STIR to be completed by the end of this year and although it currently would only work with VoIP technology, the CRTC expects providers to develop a comparable solution for traditional telephone service. Accordingly, by March 31, 2019, the CRTC expects that Canadian telecommunications service providers “will implement measures to authenticate and verify caller ID for all IP-based voice calls” and that the industry will establish an entity to administer the certification process. Providers must also begin reporting on progress every six months and report on the percentage of calls using the process.

Another aspect of the problem in reducing unlawful robocalling is identifying where the call actually originates—something called traceback. This is complicated because the call may traverse many carriers’ networks and tracing the call can be an intensive manual process, especially when the call starts in a foreign country. The CRTC notes, nevertheless, that the UK has adopted a national standardized traceback process and that a similar process is under consideration here in the U.S., citing a [study](#) by the Robocall Strike Force. The CRTC directs one of its

February 6, 2018

advisory committees, similar to one that advises the FCC on technical network matters, to “develop an industry-wide call traceback process and file a report regarding such a process” within nine months.

Given the mounting frustration in the U.S. over these unlawful calls, and the steps already started by the FCC, it would not be surprising to see the FCC attempt to accelerate progress on U.S. adoption of similar measures. This would require significant industry cooperation and may stress the resources of smaller providers. Questions regarding how to pay for the system must also be addressed.

Michael Pryor

Shareholder

mpryor@bhfs.com

202.383.4706

This document is intended to provide you with general information regarding regulations involving caller authentication technology. The contents of this document are not intended to provide specific legal advice. If you have any questions about the contents of this document or if you need legal advice as to an issue, please contact the attorneys listed or your regular Brownstein Hyatt Farber Schreck, LLP attorney. This communication may be considered advertising in some jurisdictions.