SUPER CHANNEL™
Entertainment Network

March 15, 2021

Mr. Claude Doucet,
Secretary General,
CRTC,
Terrasses de la Chaudière
Central Building,
1 Promenade du Portage,
Gatineau, Quebec K1A 0N2

filed via GCKey

Dear Mr. Doucet.

re: Compliance and Enforcement and Telecom Notice of Consultation CRTC 2021-9

1. This intervention is filed on behalf of Allarco Entertainment 2008 Inc. ("Allarco"). Allarco[1] operates the national English-language pay television discretionary service *"Super Channel*".

2. Super Channel and many other Canadian discretionary services, have had their programming pirated by individuals and corporate entities (the "Signal Pirates") who provide end-users with digital (android) set top boxes, that utilize software applications to illegally intercept streams of programming, and / or to access streams of pirated programming hosted and illegally streamed by pirate organizations.

3. The pirated programming is streamed, through the use of servers located within Canada or overseas.

4. The Signal Pirates, without the consent or authority of the Canadian broadcaster, re-sell the programming by way of monthly subscriptions, with no funds remitted to the lawful rights holders, *i.e.* Super Channel. In other cases, the pirated programming is made available at no additional charge to the end user, after the purchase of certain set top boxes.

5. In some cases, parties engaged in piracy, front-end-load their profit, from the sale of the set top box at a premium price, which results in the Signal Pirates deriving illegal revenue from making the pirated streams available. In other scenarios, software is provided to end-users in the form of applications, that enable the consumers to receive Super Channel and such other Canadian services, or their programming, without payment of legitimate subscription fees.

[1] Licensee of Super Channel: Allarco Entertainment Limited Partnership

6. Pirate streams also consistently remove commercials and broadcasters' promotional messages ("Coming next week on Super Channel…"). Allarco's investigations also showed that pirates are increasingly selling and injecting their own commercials into pirated streams. Piracy is big business worth billions, with multiple profit models derived from the sale of pirate devices, and pirate software in addition to the sale of pirated programming.

7. In September 2019, Allarco filed a lawsuit against four major Canadian retailers alleged to have been complicit in the promotion of the downloading and illegal streaming of content on Pirate Devices.

8. The defendants sold devices that are *"designed or produced primarily for the purposes of circumventing a technological protection measure*", and/or "the uses or purposes of which are not commercially significant other than when used for the purposes of circumventing a technological protection measure."

9. The application by Allarco, for an injunction to protect its intellectual property from theft, was argued before the Alberta Court of Queen's Bench on March 2, 2021.

10. Prior to filing the lawsuit, Allarco and its legal counsel retained the services of experts in the field of cybersecurity and cybercrime to investigate and document the specific acts of piracy. Allarco's undercover investigator, Donald Best, is a former police sergeant detective with over 35 years of experience, including piracy investigations since 1996. His evidence and investigation were foundational in the 2004 Supreme Court of Canada satellite piracy case 'Bell ExpressVu Limited Partnership v. Rex'. In the last 3 years, Mr. Best purchased several hundred pirate devices from retail stores and suppliers across Canada.

11. Laboratory examinations of devices purchased by Mr. Best were initially conducted by Rippul Cyber Security Services in Ontario. Dr. Eric Cole, conducted further examinations of the Pirate Devices, confirming the work and laboratory standards of Allarco's experts, and conducting new examinations of additional devices.

12. Appended to this intervention at Exhibit 1, is the affidavit of Dr. Eric Cole, PHD, a court-acknowledged expert in information technology with a focus on cyber security, secure network design, perimeter defense, vulnerability discovery and intrusion of detection systems. Dr. Cole served as a Commissioner on Cyber Security, in the administration of President Obama.

13. Dr. Cole determined that various Pirate Devices which were examined, exhibited invasive and/or potentially malicious behaviors including:
    - "secret network scanning and probing of computers and other local network devices - specifically targeting Microsoft file sharing and files (File types include Word documents, databases, spreadsheets, PDFs, audio, video, images and all other types of electronic files residing on computers, network-attached hard drives, and other connected devices);

- Reporting to unknown servers in China, compromising information about the Pirate Device such as its location, software load, security level, running programs and the structure of the local network the device is attached to;

- Deception and evasion techniques are used to secretly exfiltrate information to servers in China. These techniques are used to circumvent Data Loss Prevention scanning by network protection firewalls.[2]"

14. Dr. Cole also stated that the Pirate Devices transmitted to servers in China, IP addresses that can be used for geo-location and can be used to find out the location of an entity, device, or other attributes of a business or home Internet connection.

15. Dr. Cole also noted that, as a former member of the CIA and Cybersecurity Commission to the President of the United States, he is aware that *"for many decades the People's Republic of China ('PRC') has been a major nation-state player in the use of espionage to further its strategic, economic and political agendas and goals."* He believes that the malicious behaviors of the devices would be of concern to any Canadian with a Pirate Device attached to their home, business or organization computer network.

16. Dr. Cole's observations concerning devices reporting to China without notice to the end user were confirmed by experts from Ernst and Young who filed an affidavit for defendants in the Allarco lawsuit. Attached at Exhibit 2, are excerpts from the Expert Report of Joseph Pochron of Ernst and Young LLP (*"Incoming and outgoing connections to Locations in China and other countries*") filed July 15, 2020 in the Court of Queen's Bench of Alberta – showing secret China communications.

17. Although TNC CRTC 2021-9, references botnets, - as networks of malware-infected computers that are under the control of a command-and-control server, operated by a malicious actor, we believe that the Pirate Devices utilized to intercept the program content of Super Channel and other Canadian discretionary programming services, exhibit many of the same attributes. Canadian consumers are largely unaware that the Pirate Devices, can acquire access to their computers, hard drives, home networks, and other (connected) devices within their homes or businesses. These devices can also acquire, and transmit to those off-shore servers, files, documents and other personal information. Consequently, the key questions posed by the Commission, in reference to botnets, are relevant to the sale and deployment and operation of Pirate Devices, described above.

18. Further, Allarco's investigations and research reveals direct connections between the use of botnets and piracy of broadcast programming. Not only are botnets used to steal and distribute pirated programming, piracy becomes a trojan horse and vector through which the botnets expand their illicit networks used to distribute malware, and carry out Denial of Service attacks and other nefarious purposes. The commercialization of piracy is greatly aided by botnets.

[2] Dr. Eric Cole Affidavit - Paragraph 22.

19. Exhibit 2, provides a listing of several hundred outgoing connections including IP address and destination countries for the MyGica 1900 Pro set top box, on the first launch of the Kodi application. **Various servers and their locations in China are highlighted in yellow.** Note that some of the destinations include IP addresses at universities or schools located in Maryland U.S.A. (University of Maryland); Denmark (Danmarks Tekniske Universitet); Sweden (Umea University); India (nr. Monal Public School); Computers, and servers at these locations may be connected to the set-top Pirate Devices, as botnets.

20. Below, we are responding to the Commission's questions.

21. Q1. Allarco's response to question 1, is in the affirmative. If TSPs or ISPs blocked Pirate Device communication, two goals would be achieved. First, would be to curtail the theft of intellectual property within Canada, which is facilitated through the operation of the Pirate Devices. Second, would be to curtail the malicious transmission of personal data, personal files, and other information to servers located outside of Canada (i.e. China). Allarco, also believes that by blocking communications to and from the Pirate Devices, the off-shore network operators would be unable to infiltrate (Canadian) users' other devices, including hard drives, computers and networks which are connected to the same in-home or office networks. The blocking of the Pirate Devices, and hence, blocking of spyware, malware, etc., is warranted, and would not undermine the overall precepts of network neutrality.

22. Q.2. Allarco expects that TSPs and ISPs will address the issue of Internet service subscribers' privacy in their submissions. We intend to reserve the opportunity to address this issue in the reply phase of this proceeding.

23. Q3. Allarco's response to question 3, is that Canadian consumers should not have the ability to *"opt out"* of blocking programs, where Pirate Devices are in use. The entire purpose of the Pirate Device, is to circumvent copyright law and to steal intellectual property. It has been Allarco's experience that in many cases Canadian consumers who purchase the Pirate Devices from retail outlets are not informed that the devices intercept and thereby steal copyrighted content. Some Pirate Device sellers misinform Canadian consumers that using the devices to 'steal' programming is not illegal. If due to implementation of a blocking framework, the Pirate Devices were unable to connect to servers containing the pirated intellectual property, members of the public would suffer no direct harm.

24. Q4. Allarco concurs with the Commission that an independent party with expertise in cyber security would be best suited to assess the impact of blocking a particular domain or IP address, and to decide whether blocking is warranted. Allarco has employed the services of cyber security experts, and would seek to assist such an independent party, by presenting accurate and factual data, pertaining to the IP address(es), identity and location of foreign servers, etc.

25. Q5. Allarco does not believe an "opt in" program would be warranted, with respect to the blocking of Pirate Devices. The deployment and use of these Pirate Devices are for the primary purpose of facilitating illegal access to intellectual property. We would not foresee any circumstance, where a purchaser (or user) of a Pirate Device, should have the right to "opt out" of blocking.

26. Q.6. We do not foresee the probability of over blocking or false positives, with respect to blocking communications to/from Pirate Devices. In the scenario presented in Q.4, we would anticipate that Allarco or another rights holder of intellectual property would be required to provide the independent expert evidence that the IP addresses to be blocked are being used to transmit malware, or those foreign servers are being used to facilitate illegal access to the copyright protected program content. Similarly, the proponents of blocking would be required to demonstrate to the independent expert, the technical method(s) by which data is surreptitiously acquired from Canadians using Pirate Devices, and transmitted to servers located outside of Canada. Since the Pirate Devices, are generally single-purpose devices, we would not foresee situations where the consumer is precluded from carrying out lawful activities, on their other (lawful) streaming devices (e.g. Roku, AppleTV, Amazon FireTV) in their homes or offices, or impact their ability to use their computers, tablets or mobile phones for such purposes as web-surfing, email, video-conferences, etc.

27. Q7-Q10 inclusive. Allarco has no definitive response at present. Allarco is neither an ISP nor a TSP, so we have no expertise in respect of blocking techniques which could be implemented by an ISP or TSP. Allarco reserves the right to comment on filings by TSPs and ISPs and other intervenors at the reply phase.

28. Allarco believes that the cost to the Canadian economy, through the use of the Pirate Devices, amounts to several billion dollars per year. In 2017, it was estimated that android devices had deployment in 7% of Canadian homes.[3] The losses to the Canadian broadcasting system, in 2017 would have been approximately $125 million per month – or $1.5 Billion annually. Since that time the number of households using Pirate Devices in Canada has increased significantly. Piracy is not a victimless crime. The sale and use of Pirate Devices, undermines the Canadian broadcasting system and the *Telecommunications Act*. As a result, Canadian broadcast licensees are deprived of revenue. This includes Canadian BDUs, who provide these discretionary television services, to Canadian subscribers. Millions of dollars of taxes, which would otherwise be collected from subscription sales, are lost, due to piracy. There is a trickle-down effect of widespread piracy. Canadian broadcasters, through their conditions of licence, spend a significant percentage of their gross revenue for the purchase of Canadian programs. The leakage of hundreds of millions of dollars of annual revenue out of the Canadian broadcasting system, due to widespread signal piracy and the use of Pirate Devices impacts the creative community. Moreover, the proliferation of malware, through Pirate Devices, has the potential to severely undermine the personal privacy of Canadians. Installation of malware, can also lead to identity theft, compromise of

[3] Reference: Exhibit 3 – Paragraphs 42-43 – Affidavit of Donald Best.

individuals' passwords, and may result in the fraudulent use of personal information, by way of illegal access to personal financial records, credit cards, and other accounts.

29. While it is difficult to quantify pirating losses to the Canadian content creation and broadcasting industries, Allarco believes that the cost to the Canadian economy, through the use of the Pirate Devices, amounts to at least several hundred million dollars per year if not considerably more. As shown in the Federal Court of Canada case 'VaderStreams.ca' as documented in the January 3, 2020 affidavit of Donald Best (paras 21 to 23), the Canadian website VaderStreams.CA had over 8 million subscribers, each paying about CDN$53.73 every three months for annual gross pirating revenues of CDN$1.72 billion dollars. That was just one Canadian pirating organization with over 8 million subscribers primarily in Canada and the USA.

30. Further, please see paragraphs 32 through 37 of the Affidavit of Donald Best (Exhibit 3 – attached), referencing Telecom Decision CRTC 2018-384, and the 2019 U.S. Chamber of Commerce Study, "*Impacts of Digital Video Piracy on the U.S. Economy*". Each document provides further context as to the financial impact of piracy.

31. Allarco appreciates the opportunity to participate in this proceeding. We look forward to reviewing submissions of other stake-holders and providing reply comments during the subsequent phase of this proceeding.

Yours truly,

Don McDonald
President & CEO
Allarco Entertainment 2008 Inc.

Attachments:

Exhibit 1: The Affidavit of Dr. Eric Cole, PHD
Exhibit 2: Excerpts from the Expert Report of Joseph Pochron of Ernst & Young LLP - *"Incoming and outgoing connections to Locations in China and other countries*"
Exhibit 3: Excerpts from the Affidavit of Donald Best.

- End of Document -