PUBLIC

CT-2002-002

THE COMPETITION TRIBUNAL

IN THE MATTER OF the *Competition Act*, R.S.C. 1985, c. C-34;

AND IN THE MATTER OF the proposed acquisition by Rogers Communications Inc. of Shaw Communications Inc.;

AND IN THE MATTER OF an application by the Commissioner of Competition for one or more orders pursuant to section 92 of the *Competition Act*.

B E T W E E N:

COMMISSIONER OF COMPETITION

Applicant

- and –

ROGERS COMMUNICATIONS INC. and SHAW COMMUNICATIONS INC.

Respondents

- and -

THE ATTORNEY GENERAL OF ALBERTA and VIDEOTRON LTD.

Interveners

WITNESS STATEMENT OF RON MCKENZIE

I, Ron McKenzie, of the City of Toronto, in the Province of Ontario, STATE AS FOLLOWS:

1. I am the Chief Technology and Information Officer at Rogers Communications Inc. ("**Rogers**"). Between June 2021 and July 2022, I was President, Rogers for Business responsible for delivering Wireless, Wireline, Internet of Things, Advanced

Services and Data Centre products and solutions to small, medium, large and public sector businesses across Canada.

2. Prior to assuming my role as President, Rogers for Business, I managed Technical Operations for more than two years, where I was responsible for Install, Service & Maintenance, and Technical Support for both Wireless and Wireline. This role included managing Rogers' response to the Covid-19 pandemic and the impact increased usage had on our network and business overall.

3. I have worked in the technology and telecommunications industry for more than 30 years across Canada and the United States. Prior to joining Rogers, I worked for more than 10 years at Shaw Communications in roles of increasing responsibility, ultimately leading operations as the Chief Operating Officer, and as the executive lead of Business. I graduated with a BASc in Electrical Engineering from the University of Toronto in 1984 and attended the CTAM Cable Executive Management program at the Harvard Business School in 2014.

4. I have reviewed the public versions of the September 23, 2022 witness statements of Stephen Howe and Nazim Benhadid.

Response to Mr. Howe's statement

5. At paragraph 16 of his statement, Mr. Howe refers to Bell's "wireless and wireline networks" using different network infrastructures. The statement appears to suggest that Bell's wireless and wireline networks do not share a common or "converged" IP core.

6. Based on my experience, this is not accurate. The networks of Bell and Telus, like Rogers, each have a common or converged core. This means that, like Rogers, Bell's wireless and wireline traffic flows through a common or converged IP core. To my knowledge, substantially all telecommunications providers worldwide operate on the basis of a converged wireless and wireline core. Similarly, Rogers has the same 'highly survivable routing exchange architecture' as Bell and uses the same or similar equipment.

7. In paragraph 16 and thereafter, Mr. Howe states that Bell engineers its networks and directs its investments to support network reliability and resiliency. So does Rogers. We have a 100% redundant core network with geographic diversity and multiple transport paths connecting the core network across Canada. We also support network resiliency through people and processes in many of the same or similar ways as Mr. Howe describes. Unfortunately, these features of network resiliency and network architecture did not prevent the July 8 wireless and wireline outage, described below, and they would not have prevented a wireless and wireline outage at any provider with a converged IP core.

The July 8 Network Outage & New Network Resiliency Measures

8. On July 8, 2022, Rogers experienced a network outage that affected wireless and wireline services across Canada.

9. The outage was caused by a coding error following an update to the core network. The circumstances of this outage have been accurately described publicly in hearings before Parliament's Standing Committee on Industry and Technology ("**INDU**")

and in response to requests for information from the CRTC. A redacted copy of Rogers' first letter to the CRTC describing the outage is attached as **Exhibit 1.**

10. In substance, the coding error deleted a routing filter and allowed for all possible routes to the Internet to pass through the routers. As a result, the routers began propagating abnormally high volumes of routes throughout the core network. Certain network routing equipment became flooded, exceeded their capacity levels and were then unable to route traffic, causing the common core network to stop processing traffic. As a result, the Rogers network lost connectivity to the Internet for all incoming and outgoing traffic for both the wireless and wireline networks for our consumer and business customers.

11. On July 25, 2022, I attended an INDU Committee Hearing together with Rogers' Chief Executive Officer, Anthony Staffieri. The INDU hearing provided Rogers with an opportunity to explain the steps that we are taking to prevent future system-wide network outages. A copy of Mr. Staffieri's opening remarks to INDU are attached as **Exhibit 2**. Among other things, Rogers has committed to the following network resiliency measures:

(a) A $286 million logical and physical separation of Rogers' wireless and wireline networks by splitting Rogers' IP core, so that if one network were to experience a system-wide outage in the future, it would not cause a material service interruption to the other;

(b) A review of Rogers' policies and procedures in reviewing, testing and implementing code during network maintenance updates; and

(c) a Memorandum of Understanding between telecommunications carriers that will allow them to more effectively work together in the event of an emergency, including to ensure that the 9-1-1 system is not vulnerable to an outage or other network disruption. This Memorandum of Understanding was finalized and delivered to ISED on September 7, 2022, a copy of which is attached as **Exhibit 3**. Rogers, Videotron, Shaw, Bell and Telus are among the twelve signatories.

12. The physical and logical separation of Rogers' wireline and wireless networks is a key aspect of Rogers network resiliency plans and is unprecedented in the Canadian telecommunications industry.

13. Rogers remains committed to ensuring that we continue to provide Canadians with the fast and reliable connectivity that we have delivered over the past four decades.

Response to Mr. Benhadid's statement

14. At paragraph 4 to 6 of his statement Mr. Benhadid suggests that wireline network ownership is critical to wireless network performance and reliability. I disagree. And, while I understand this issue will be dealt with elsewhere in evidence, I will make two comments. First, his assertion is inconsistent with my own experience in the industry, and with the acknowledged fact that neither Bell nor Telus own a wireline network that covers the entirety of their respective wireless footprints. Second, and related, TELUS leases about [redacted] wireline circuits from Rogers, at a cost of about [redacted] per month.

SWORN by Ron McKenzie at the City of Toronto, in the Province of Ontario, before me on October 21, 2022 in accordance with O. Reg. 431/20, Administering Oath or Declaration Remotely.

Commissioner for Taking Affidavits
(or as may be)

BRADLEY VERMEERSCH

RON MCKENZIE

This is **Exhibit "1"** referred to in the Affidavit of Ron McKenzie affirmed by Ron McKenzie at the City of Toronto, in the Province of Ontario, before me on October 20, 2022 in accordance with O. Reg. 431/20, Administering Oath or Declaration Remotely.

Commissioner for Taking Affidavits (or as may be)

BRADLEY VERMEERSCH

Abridged

July 22, 2022

Filed via GCKey

Mr. Claude Doucet
Secretary General
Canadian Radio-television and
Telecommunications Commission
1 Promenade du Portage
Ottawa, ON K1A 0N2

Dear Mr. Doucet:

RE: Rogers Canada-wide service outage of July 2022

Rogers Communications Canada Inc. ("Rogers") is in receipt of a letter containing Requests for Information ("RFIs") from the Canadian Radio-television and Telecommunications Commission ("CRTC" or the "Commission"), dated July 12, 2022, concerning the above-mentioned subject. Attached, please find our Response to that letter.

At the outset, Rogers appreciates the opportunity to explain to the Commission, the Government of Canada and all Canadians what transpired on July 8th, 2022. The network outage experienced by Rogers was simply not acceptable. We failed in our commitment to be Canada's most reliable network. We know how much our customers rely on our networks and we sincerely apologize. Rogers is particularly troubled that some customers could not reach emergency services or receive alerts during that outage.

We have identified the cause of the outage to a network system failure following an update in our core IP network during the early morning of Friday July 8th. This caused our IP routing network to malfunction. To mitigate this, we re-established management connectivity with the routing network, disconnected the routers that were the source of the outage, resolved the errors caused by the update and redirected traffic, which allowed our network and services to progressively come back online later that day. While the network issue that caused the full-service outage had largely been resolved by the end of Friday, some minor instability issues persisted over the weekend. The network is now fully operational and working to the high standards that our customers expect.

This outage caused real pain and significant frustration for everyone. Canadians were not able to reach their families. Businesses were unable to complete transactions. And critically, some emergency and essential calls could not be completed. We let people down and we are crediting all our customers the equivalent of five (5) days of service. This credit will be automatically applied to all customer accounts.

Since the outage, our customer service representatives have been working around the clock and have caught up on the backlog of issues. We are also proactively reaching out to the major organizations that depend on our services, including governments, public institutions and corporate enterprises, in order to answer their questions.

It is clear that what matters most is that Rogers ensures this does not happen again. We are conducting

a full review of the outage. Our engineers and technical experts have been and are continuing to work alongside our global equipment vendors to fully explore the root cause and its effects. We will also increase resiliency in our networks and systems which will include fully segregating our wireless and wireline core networks. Lastly, we have additionally hired an external review team to further assess and provide insights into the outage. This will involve a complete evaluation of all our processes, including the performance of network upgrades, disaster recovery procedures, and communication with the public.

Additionally, Rogers will work with governmental agencies and our industry peers to further strengthen the resiliency of our network and improve communication and co-operation during events like this. Most importantly, we will explore additional measures to maintain or transfer to other networks 9-1-1 and other essential services during events like these.

In order to regain the trust of Canadians, it is important that we provide open answers to the questions that they have about the outage. That is why when answering the CRTC RFIs, Rogers is being as transparent as possible. However, with that being said, Rogers must also ensure that all commercially and operationally sensitive information remains confidential. This is particularly true for systems designs and network operations that could be exploited by malicious actors who seek to disrupt our systems.

Rogers therefore requests that the CRTC treat certain information contained in this Response as **confidential**, pursuant to subsection 20(1)(b) of the *Access to Information Act*, and sections 38 and 39 of the *Telecommunications Act*. For competitive reasons, and also to protect our customers as well as our networks and vendors, Rogers would never publicly disclose some of the information contained in this Response other than to the Commission. Some of the information submitted contains highly sensitive information about Rogers' networks and operations. Rogers submits that any possible public interest in disclosure of the information in this Response is greatly outweighed by the specific direct harm that would flow to Rogers and to its customers. Rogers is also filing an abridged version of this Response, except for six appendices since they are confidential in their entirety.

Below, Rogers will address in detail each of the individual requests for information posed by the CRTC.

Sincerely,

Ted Woodhead
Chief Regulatory Officer & Government Affairs

Attach.

cc: Fiona Gilfillan, CRTC, fiona.gilfillan@crtc.gc.ca
Michel Murray, CRTC, michel.murray@crtc.gc.ca

Q1.
Current Outage

Provide a complete and detailed report on the service outage that began on 8 July 2022, including but not limited to:

A.
Rogers requests that the CRTC treat certain information contained in this Response as **confidential**, pursuant to subsection 20(1)(b) of the *Access to Information Act*, and sections 38 and 39 of the *Telecommunications Act*. For competitive reasons, and also to protect our customers as well as our networks and vendors, Rogers would never publicly disclose some of the information contained in this Response other than to the Commission. Some of the information submitted contains highly sensitive information about Rogers' networks and operations. Rogers submits that any possible public interest in disclosure of the information in this Response is greatly outweighed by the specific direct harm that would flow to Rogers and to its customers.

(i) status to date and all relevant timelines (including details of actions taken, what unfolded and what were the results, factors that contributed to the outage and led it to become progressively worse, and why could steps not be taken to contain the outage before it impacted more services such as Interac and others);

To assist the Commission and help inform the public, Rogers is providing both a high-level overview of the July 8th outage as well as a more technical account of the incident. This includes a detailed timeline of the outage and recovery, which is provided as an attachment titled "CONFIDENTIAL_Rogers(CRTC)11July2022-1_i_Appendix".

The Planning Process
The network outage experienced by Rogers on July 8th was the result of a network update that was implemented in the early morning. The business requirements and design for this network change started many months ago. Rogers went through a comprehensive planning process including scoping, budget approval, project approval, kickoff, design document, method of procedure, risk assessment, and testing, finally culminating in the engineering and implementation phases. Updates to Rogers' core network are made very carefully.

The Implementation
The update in question was the sixth phase of a seven-phase process that had begun weeks earlier. The first five phases had proceeded without incident. On the morning of Friday July 8th, 2022, the implementation of this sixth phase started at 2:27AM EDT. Maintenance and update windows always take place in the very early morning hours when network traffic is at its quietest. At 4:43AM EDT, a specific coding was introduced in our Distribution Routers which triggered the failure of the Rogers IP core network starting at 4:45AM.

The Outage

The configuration change deleted a routing filter and allowed for all possible routes to the Internet to pass through the routers. As a result, the routers immediately began propagating abnormally high volumes of routes throughout the core network. Certain network routing equipment became flooded, exceeded their capacity levels and were then unable to route traffic, causing the common core network to stop processing traffic. As a result, the Rogers network lost connectivity to the Internet for all incoming and outgoing traffic for both the wireless and wireline networks for our consumer and business customers.

Specifically, the outage unfolded as follows:

[redacted]

While every effort was made to prevent and limit the outage, the consequence of the coding change affected the network very quickly.

[redacted]

The Recovery

To resolve the outage, the Rogers Network Team assembled in and around our Network Operations Centre ("NOC") and re-established access to the IP network. They then started the detailed process of determining the source of the outage, leading to identifying the three

Distribution Routers as the cause. Once determined, the team then began the process of restarting all the Internet Gateway, Core and Distribution Routers in a controlled manner to establish connectivity to our wireless (including 9-1-1), enterprise and cable networks which deliver voice, video and data connectivity to our customers. Service was slowly restored, starting in the afternoon and continuing over the evening. Although Rogers continued to experience some instability issues over the weekend that did impact some customers, the network had effectively recovered by Friday night.

Rogers more detailed activities to recover the network were as follows:

[redacted]

[redacted]

(ii) what was the root cause of the outage (including what processes, procedures or safeguards failed to prevent the outage, such as planned redundancy or patch upgrade validation procedures);

Like many large Telecommunications Services Providers ("TSPs"), Rogers uses a common core network, essentially one IP network infrastructure, that supports all wireless, wireline and enterprise services. The common core is the brain of the network that receives, processes, transmits and connects all Internet, voice, data and TV traffic for our customers.

Again, similar to other TSPs around the world, Rogers uses a mixed vendor core network consisting of IP routing equipment from multiple tier one manufacturers. This is a common

industry practice as different manufacturers have different strengths in routing equipment for Internet gateway, core and distribution routing. Specifically, the two IP routing vendors Rogers uses have their own design and approaches to managing routing traffic and to protect their equipment from being overwhelmed. In the Rogers network, one IP routing manufacturer uses a design that limits the number of routes that are presented by the Distribution Routers to the core routers. The other IP routing vendor relies on controls at its core routers. The impact of these differences in equipment design and protocols are at the heart of the outage that Rogers experienced.

The Rogers outage on July 8, 2022, was unprecedented. As discussed in the previous response, it resulted during a routing configuration change to three Distribution Routers in our common core network. Unfortunately, the configuration change deleted a routing filter and allowed for all possible routes to the Internet to be distributed; the routers then propagated abnormally high volumes of routes throughout the core network. Certain network routing equipment became flooded, exceeded their memory and processing capacity and were then unable to route and process traffic, causing the common core network to shut down. As a result, the Rogers network lost connectivity internally and to the Internet for all incoming and outgoing traffic for both the wireless and wireline networks for our consumer and business customers.

To assist the Commission, the root cause is described in more detail below:

[redacted]

(iii) which Rogers companies and services were impacted and how;

Since the outage was to Rogers' core network, all of Rogers' services by all our brands (including Fido and Chatr) were impacted. Our wireless (voice, text and data), home phone telephony, Internet and TV services were down during the outage.

Note that some wireless customers had intermittent service(s) (e.g. texting and 9-1-1 access) throughout the day on our GSM and 3G networks [redacted]

Rogers Bank:
The July 8th outage impacted Rogers Bank (the "Bank") employees as the Bank's corporate network, Virtual Private Network ("VPN"), and telephone services (all provided and operated by Rogers) were all impacted. As a result, Bank employees utilized non-Rogers Internet and phone services so that they could log into and monitor the Bank systems.

The impact to the Bank's customers was minimal as the Bank services were available and the Bank's customers were able to transact on their Rogers Bank credit cards. There was no interruption in the Bank's core systems (credit card processing, Interactive Voice Response ("IVR"), Call Centre and customer self-serve mobile application) and these core systems remained available to the Bank's customers. No critical Bank systems were impacted, and all daily processing was completed as required, including by the Bank's statement printing vendor and its card personalization bureau which received their daily files and were processing them per standard service level agreements and procedures.

The only customer-facing service that was unavailable was the Bank website (hosted by Rogers), which impacted the ability of potential Bank customers to apply for a Bank credit card. The Bank's customers could still call into the Bank's call center for account servicing. Access to the Bank's website was not available from 4:00AM EDT on July 8th to 1:00AM EDT on July 9th.

If the Bank's customers contacted the Bank's contact center and stated that they were unable to make a payment to their Rogers Bank credit card from their financial institution on July 8th due to having no Internet and/or phone service, the Bank's customer contact center would provide adjustments or client service gestures, as appropriate to the situation, in accordance with the Bank's existing complaints resolution process.

Rogers Media's broadcasting services were impacted as follows:

- CISW-FM (Whistler) and CJAX-FM-1 (Whistler) and CISP-FM (Pemberton) were unable to transmit programming for approximately 22 hours due to [redacted]

[redacted]

- CHYM-FM, CIKZ-FM, CKGL-FM (Kitchener) could not transmit programming from 4:45AM EDT to 5:04AM (19 minutes) until back up system was operationalized using an alternate Internet connection. [redacted]
- CHST-FM (London) was not able to air live programming from 4:45AM EDT to 1:02PM on the same day. During that time, evergreen programming was aired from an MP3 player at the base of the transmitter until our engineering team was able to establish a connection between the studio and transmitter site using an alternate Internet connection. [redacted]
- CKOT-FM and CJDL-FM (Tillsonburg) were not able to air live programming from 4:45AM EDT to 10:58PM on the same day. During that time, evergreen programming was aired from an MP3 player at the base of the transmitter until an Internet connection was re-established between the studio and the transmitter site. [redacted]
- OMNI Regional was unable to produce three of its national newscasts (Arabic, Punjabi, Filipino) on July 8th. The in-house programming tool used to produce these programs (Inception) is [redacted] and was not available to the production teams during the outage. As a result, OMNI Regional was unable to comply with condition of licence 12 related to the exhibition of national newscasts. [redacted]
- Closed captioning for live events aired on Sportsnet on July 8th was not available due to captioners use of encoders that relied on Rogers' phone lines/SIP lines that were impacted as a result of the outage. Closed captioning for Citytv's live programming was not impacted as redundant landlines were in place that allowed captioners to establish connection. [redacted]

(iv) which other telecommunications service providers (TSPs) were impacted and how;

As a wholesale provider of telecommunications services in Canada, several other carrier using Rogers' networks were impacted by the outage.

The following TSPs use our wireless network in some form to communicate and to operate their networks. Therefore, the following companies were impacted: [redacted]

Similarly, all our roaming partners in Canada would have been affected when attempting to roam on Rogers' network [redacted]

[redacted] as well as all our international roaming partners.

Finally, all Third-Party Internet Providers ("TPIA") who utilize Rogers to provide Internet services to their customers would have experienced a full outage. Rogers has [redacted]

(v) total number of customers impacted, broken down by province, by TSP (for Rogers and each of its affiliates, for each wholesale customer, others), and, where possible, by type of end-customer (residential or personal, small business, all other businesses/enterprises);

As mentioned above, all our residential (cable and wireless) as well as our wholesale customers were impacted on July 8th. The table below presents a split per province and per customer type:

[redacted]

(vi) impact on federal, provincial, territorial and municipal government services;

Rogers has several federal, provincial, territorial and municipal customers across the country which were impacted during the July 8th outage. We provide various types of services to these customers, including but not limited to wireline, wireless, long-distance, SIP, toll-free, and M2M.

Below is a list of these critical customers. It is important to note that in most of the cases, we provide a portion of the telecommunications solution, but not all underlying services. Many institutional customers have redundant services:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

(vii) a description of the extent of the Interac outage (e.g. only for businesses who had Rogers as their service provider or broader) and extent to which any other critical infrastructure sectors (e.g. health, transportation, energy, etc.) were affected;

[redacted]

Aside from Interac, Rogers provides wireless and wireline connectivity services to various customers who are classified as critical infrastructure (e.g. hospitals, gas and energy providers, etc.). Each of these customers' services were impacted by the outage. It is not known whether these customers were fully impaired or if they had some degree of dual-carriers diversity that protected them from full disablement. Rogers has approximatively [redacted] of these customers across the country. As described in Rogers(CRTC)11July2022-1.viii below, Rogers prioritizes reinstating services with these important customers. Below is a list of our major accounts (excluding Emergency and Police accounts, which are discussed in Rogers(CRTC)11July2022-1.vi above):

[redacted]

[redacted]

[redacted]

(viii) how did Rogers prioritize reinstating services and what repairs were required;

Rogers' priority sequence for service restoral was as follows:

[redacted]

[redacted]

The prioritization of service restoration was always dependent on which service was most relied upon by Canadians for emergency services. As wireless devices have become the dominant form of communicating for a vast majority of Canadians, the wireless network was the first focus of our recovery efforts. Subsequently, we focused on landline service, which remains another important method to access emergency care. We then the worked to restore data services, particularly for critical care services and infrastructure.

(ix) what measures or steps were put in place in the aftermath of the earlier-mentioned April 2021 outage, and why they failed in preventing this new outage;

In April 2021, Rogers experienced a network-wide wireless outage for almost 22 hours. While a serious incident, it differed substantially from the outage of July 8th. Unlike the recent outage, which affected Rogers' core network and thereby impacting wireless, wireline and Internet services, the 2021 outage was strictly affected the wireless network. [redacted]

Measures Taken Since April 2021:

Since April 2021, we have taken the following steps to improve our wireless network resiliency and operations:

[redacted]

Additionally, the follows steps and guidelines were put in place:

Taken together, Rogers instituted multiple measures to prevent a recurrence of the April 2021 outage. While some of these steps were broad in nature and will help prevent any type of incident, many were also focused on the particular circumstances of what happened in 2021. Unfortunately, they did not prevent the particular circumstances that resulted in the July 8th outage, although they did contribute positively to its resolution.

In order to provide the Commission with more details of the measures taken after the 2021 outage, we have attached a detailed Appendix entitled "CONFIDENTIAL_Rogers(CRTC)11July2022-1_ix_Appendix".

(x) what measures or steps Rogers has, or plans to, put in place to prevent issues such as those that led to this incident going forward, as well as the timelines for any future measures to be put in place;

Rogers has already taken steps in order to prevent another outage. We have developed very specific measures, for the immediate term, short term and medium term, that will be implemented in the coming days, and weeks. Here is a summary of our action items:

[redacted]

[redacted]

Most importantly, Rogers is examining its "change, planning and implementation" process to identify improvements to eliminate risk of further service interruptions. These include the following steps:

[redacted]

(xi) what is Rogers' internal process for conducting major network upgrades including governance and accountability for major engineering decisions;

The Rogers Core Engineering team follows an extremely detailed guideline, as stated in the Network Program Framework (for more details, see the attached Appendix entitled "CONFIDENTIAL_Rogers(CRTC)11July2022-1_xi_Appendix"). It is important to note that, on average, [redacted] of all requested changes are being rejected throughout this process, so that specific solution designs and related network architecture can be improved.

From the Concept/Definition Phase through to Project Closure, Rogers uses a "Stage Gate" framework that defines progressively elaborated commitments for managing the introduction of changes in our networks.

[redacted]

Concerning the July 8th outage, the proposed activities were very carefully reviewed, as we normally do with all network changes. We validated all aspects of this change. In fact, we had begun introducing this change weeks ago, on February 8th and had already implemented successfully the first five (5) phases in our core network.

(xii) how did the outage impact Rogers' own staff and their ability to determine the cause of the outage and restore services;

At the early stage of the outage, many Rogers' network employees were impacted and could not connect to our IT and network systems. This impeded initial triage and restoration efforts as

teams needed to travel to centralized locations where management network access was established. To complicate matters further, the loss of access to our VPN system to our core network nodes affected our timely ability to begin identifying the trouble and, hence, delayed the restoral efforts.

Despite these hurdles, our preestablished business continuity plans enabled staff to converge at specific rally points. Those equipped with emergency SIMs on alternate carriers that enabled our teams to switch carriers and assist in the initial coordination efforts. Further, we rapidly relocated our employees to two of our main offices in the GTA [redacted]. The critical network employees were able to gain physical access to our network equipment. Other essential employees were able to use alternate SIM cards, as per our "Alternate Carrier SIM Card Program" (described in Rogers(CRTC)11July2022-1.xiii below). Other employees were able to work from [redacted] Together, these groups were able to establish the necessary team to identify the cause of the outage and recover the network.

(xiii) what contingencies, if any, did Rogers have in place to ensure that its staff could communicate with each other particularly in the early hours of the outage;

On July 17th, 2015, the Canadian Telecom Resiliency Working Group ("CTRWG"), formerly called Canadian Telecom Emergency Preparedness Association, established reciprocal agreements between Rogers and Bell, and between Rogers and TELUS, to exchange alternate carrier SIM cards in support of Business Continuity. This is to allow TSPs to communicate within their organizations in the event of loss of their respective networks. Bell, Rogers and TELUS took the lead to provide SIM cards to all CTRWG members.

[redacted]

When it was realized that Rogers entire core network was offline, employees started swapping out our Rogers SIM cards with our alternate carrier SIM Cards. This previously established contingency plan allowed us to begin communicating within our organization in the early hours of the outage and to start restoring services.

(xiv) how does Rogers plan to improve its internal communications in light of this event;

Rogers is exploring several options to improve its internal communications in light of the outage and the impact it had on our employees. Some of the measures being considered include:

[redacted]

Together these measures will assist our employees' abilities to address critical issues under difficult circumstances and provide a level of redundant communications that will improve our response times.

(xv) what information was used to confirm the 9 July message that services had been restored and networks and systems were close to fully operational, and indicate whether this information was accurate and reliable;

As stated above, our network and technical teams determined the outage was due to a network system failure following an update in our core network, which caused some of our Distribution Routers to malfunction and propagate that malfunction across the core IP network. To restore our network, the technical teams disconnected the specific equipment causing the problem, redirected traffic and tested the stability of the network before bringing services back online over time.

Once it was confirmed that the core network was stable, Rogers' teams began to systematically reestablish IP connectivity to elements of the broader network, while continuing to manage traffic volumes. This process had to be completed methodically and carefully to ensure stability of the network in order to avoid overloading the network, which would have caused another outage. It was imperative that we completed this process and ensured the network was once again stable, before advising customers that our services were being restored.

Once the technology team confirmed stability of our core network, and that traffic volumes were returning to normal level across the network, we proceeded to inform customers that our network and systems were returning to fully operational service for the vast majority of our customers. We also notified them that some customers may experience intermittent issues, and that our technology teams are monitoring and would work to resolve any issue as quickly as possible.

These intermittent issues did persist over the weekend, impacting some customers as outstanding issues were being rectified. Those scenarios are not unusual in the wake of a major outage as service is incrementally restored. Equipment, service and traffic must be carefully monitored as issues arise and are dealt with on a case by case basis.

(xvi) provide a list, including timeline, medium and messaging of all communications efforts undertaken by Rogers to advise its customers of this service outage;

Rogers made dozens of customer communications during the outage and in the subsequent days, until July 13th. These messages were delivered via social media, media outlets, Rogers Sports & Media properties, website banners, virtual assistants, interactive voice responses ("IVR"), public service announcements and community forums. A detailed list of these messages is provided in the attached Appendix entitled "CONFIDENTIAL_Rogers(CRTC)11July2022-1_xvi_Appendix".

(xvii) how does Rogers plan to improve its communications to its customers and the general public in light of this event;

In response to the incident, Rogers activated its crisis communications plan and updated customers with accurate information regarding the outage and time to resolution, as it became available. It is important to note that until 10PM EDT on July 8th, Rogers did not have a precise time when services would be restored. From a communications standpoint, we did not want to disseminate inaccurate information suggesting otherwise.

During the outage, Rogers communicated with customers across several different channels, including social media, media outlets, Rogers Sports & Media properties, website banners, virtual assistants, interactive voice responses ("IVR"), public service announcements and community forums. In addition, Rogers' CEO conducted broadcast interviews with CP24, Global News, CTV News, BNN, and CityNews. Rogers SVP of Access Networks & Operations also conducted broadcast interviews on CBC and CityNews.

Given the extent and unique nature of this outage, Rogers will be updating our plans and procedures to ensure the following:

- Communications teams have back-up devices on alternate network that can be used in the event the Rogers networks are unavailable.
- Update policies and procedures to ensure that in the event of a network blackout there is minimal delay in posting details to customer care channels, web properties, social media, as well as public service announcements ("PSAs") across media properties.
- Increase frequency of updates to customer service channels, public service announcements, and web properties, even if there is limited or no additional information to share.
- Ensure crisis response teams have alternative method to access social media properties protected by two-factor authentication using a device on the Rogers network.
- Provide information across all customer services channels and media properties of the status of critical services (such as 9-1-1), how they may be impacted by the outage, and advice for customers.
- Ensure all statements posted to social media channels as images use ALT TEXT.

(xviii) actions taken by Rogers during this service interruption to mitigate the impact on Canadian institutions, infrastructure and customers, including in relation to emergency services;

Rogers took several measures to limit the impact of the outage and address critical needs of Canadians.

At around 6:00AM EDT, our Chief Technology and Information Officer reached out to his counterparts at Bell and TELUS, advising them of the issue and also to watch-out for possible cyber-attacks.

At 8:54AM EDT, we used various social and traditional media to notify Canadians. As mentioned in the response to Rogers(CRTC)11July2022-1.xvi above, between July 8th and July 13th, dozens of communications were delivered via social media, media outlets, Rogers Sports & Media properties, website banners, virtual assistants, interactive voice responses ("IVR"), public service announcements and community forums. Rogers also sent various communications to its employees via email, frontline knowledge management tools, and its internal intranet.

We prioritized restoration efforts of emergency services, wireless services and key infrastructure (e.g.. police, fire, hospitals, etc.). We also had teams focused on an incremental restoral of services (i.e. enabled Mobility Management Entity - "MME" - throttling, etc.) to ensure smooth recovery once core network was restored.

A full description on the impact on 9-1-1 and public alerting and the efforts to restore these essential services are fully examined in Rogers(CRTC)11July2022-2 (iv) and (xv). In summary, our Network Operations Center ("NOC") notified the ILECs (i.e. 9-1-1 Network Providers) at 8:39am EDT. In turn, the ILECs then notified the Public Safety Answering Points ("PSAPs"), as per CRTC-approved guidelines. With respect to Pelmorex (who manages and administers the National Alert Aggregation and Dissemination - "NAAD" - System), Rogers started to communicate with them at 9:25am EDT, and then formally confirmed, after the first BI alert was issued in Saskatchewan, that we were not able to distribute any alerts.

However, the primary means Rogers employed to mitigate the impact on Canadian institutions infrastructure and customers, including emergency services, was to focus on restoring the network as quickly as possible. Rogers considered throughout the day the possibility of addressing specific services (including most importantly 9-1-1) or customers. However, in each case it was clear that any change in focus or deployment of resources elsewhere would ultimately delay the recovery of the entire network, to the detriment of re-establishing emergency calling and critical services. Restoring the network was simply the best way to limit the impact of the outage.

(xix) extent to which Rogers sought or received assistance from other TSPs in addressing the outage or situation arising from the service interruption;

As we stated in Rogers(CRTC)11July2022-1.xviii above, our Chief Technology and Information Officer reached out to his counterparts at Bell and TELUS early on July 8th. Assistance was offered by both Bell and TELUS. However, given the nature of the issue, Rogers rapidly assessed and concluded that it was not possible to make the necessary network changes to enable our wireless customers to move to their wireless networks.

In order to allow our customers to use Bell or TELUS' networks, we would have needed access to our own Home Location Register ("HLR"), Home Subscriber Server ("HSS") and Centralized User Database ("CUDB"). This was not possible during the incident. Furthermore, given the national nature of this event, no competitor's network would have been able to handle the extra and

sudden volume of wireless customers (over 10.2M) and the related voice/data traffic surge. If not done carefully, such an attempt could have impeded the operations of the other carriers' networks. This possibility however will be explored though as part of the work towards the Memorandum of Understanding (for cooperation between carriers) that will be delivered in September 2022 to the Minister of ISED by CSTAC (note: work is currently underway by many of Canada's major carriers).

(xx) describe what more Rogers could have done to secure assistance from other TSPs to help address the outage;

On July 8th, Rogers promptly and diligently contacted other TSPs. We rapidly realized though that we would not be able to transfer our customers onto other wireless networks. As described in Rogers(CRTC)11July2022-1.xix above, in order to allow our customers to use Bell or TELUS's networks, we would have needed access our own network elements (e.g. HLR). This was not possible during the incident. Furthermore, given the national nature of this event, no competitor's network would have been able to handle the extra and sudden volume of wireless users (over 10.2M) and the related voice/data traffic surge.

Rogers, Bell and TELUS are presently assessing potential options and will report further findings and potential solutions per the creation of the Memorandum of Understanding that will be delivered in September 2022 to the Minister of ISED by CSTAC.

(xxi) whether any service level agreements (SLAs) were breached between specific vendors and Rogers in relation to this outage; and,

[redacted]

(xxii) whether Rogers breached any SLAs between itself and its customers (e.g. Interac, others) in relation to this outage.

There was no breach of our service agreements with our retail customers. However, in order to address our customers' disappointment with the outage, Rogers has already announced it will be crediting 5 days of service fees to its customers. This will be applied automatically to their next invoice.

[redacted]

Q2.
Impact on Emergency Services

Provide a complete and detailed report on the impact on emergency services of the outage that began on 8 July 2022, including but not limited to:

A.
Rogers requests that the CRTC treat certain information contained in this Response as **confidential**, pursuant to subsection 20(1)(b) of the *Access to Information Act*, and sections 38 and 39 of the *Telecommunications Act*. For competitive reasons, and also to protect our customers as well as our networks and vendors, Rogers would never publicly disclose some of the information contained in this Response other than to the Commission. Some of the information submitted contains highly sensitive information about Rogers' networks and operations. Rogers submits that any possible public interest in disclosure of the information in this Response is greatly outweighed by the specific direct harm that would flow to Rogers and to its customers.

(i) specific impact on emergency services including wireless public alerting and 9-1-1 and details of when access to emergency services was fully restored;

1. Impact to Public Alerting Service:

With respect to wireless public alerting service (WPAS"), the Rogers Broadcast Message Center ("BMC") platform was operable to receive alerts from Pelmorex, the WPAS administrator. However, broadcast-immediate ("BI") public alerts could not be delivered to any wireless devices across Rogers' coverage areas due to the outage. Based on a review of the alerts received into the WPAS BMC platform, the only impact occurred in the Province of Saskatchewan. There were four alerts, and associated updates, received but not delivered to wireless devices in Rogers' coverage area. There were no other alerts issued, as seen on our WPAS BMC platform.

With respect to broadcasting (cable TV/Radio) alerts, our alert hardware is connected to our IP network. Since we had no connection to the Internet on July 8th, we were unable to send out any alerts on that day in the regions that we were serving. Fortunately, other than in Saskatchewan, no other alerts were issued.

Please note that Rogers does not have any over-the-air ("OTA") TV / Radio stations in Saskatchewan.

2. WPAS Service Restore:

The ability to deliver alerts to any wireless devices across Rogers' coverage areas through the WPAS BMC platform was restored at the time of network restoration, late on Friday July 8th.

As a result, the next alert issued from NAAD on July 9th at 3:25PM CST was successfully broadcasted upon receipt.

3. Impact to 9-1-1:

Unfortunately, the outage of July 8th did impact 9-1-1 service across Rogers' service area, to both wireline and wireless services.

Wireline impact: There were approximately [redacted] 9-1-1 calls placed successfully across Rogers' network on July 8th. The typical daily average of total wireline 9-1-1 calls is [redacted] per day. Data is unavailable for unsuccessful wireline 9-1-1 calls. On July 9th, there were approximately [redacted] 9-1-1 calls placed successfully across Rogers' network.

Wireless impact: As can be seen in table below, the outage similarly affected wireless 9-1-1. Total successful calls were [redacted] the average daily amount of about [redacted] 9-1-1 calls made from Rogers wireless devices.

[redacted]

*** Verifiable data was not available for Newfoundland (i.e. where there is basic 9-1-1) and is therefore not included.*

As described further in Rogers{CRTC}11July2022-2.ix below, we are now able to confirm that some of our wireless customers were able to connect to other wireless networks and make 9-1-1 calls on July 8th.

4. 9-1-1- Service Restore:

[1] Based on discussions with PSAPs, a 30-second call duration was selected to identify successfully completed calls to a PSAP during the outage (i.e. [redacted] calls). This was to take into consideration the instability of the core network, which was impacting call completion and/or stability. Below that 30-second threshold, we consider that these were "Unsuccessful Calls". Potential event types that could result in an unsuccessful call to a PSAP include: Manual Disconnect (a common example is a pocket dial); User Equipment ("UE") phone disconnection; UE loses coverage; and UE runs out of battery.

[2] When Rogers wireless network is in a normal operating condition there is very limited to no impact to call completion and/or stability.

The ability to successfully complete 9-1-1 calls to a PSAP was restored at the time of network restoration. As mentioned in our earlier responses, the fastest way to restore 9-1-1 service was to restore the entire network.

(ii) whether the outage specifically impacted the 9-1-1 networks or only the originating networks, and if the former, how was this possible in light of resiliency and redundancy obligations imposed by the Commission;

The outage solely impacted Rogers' originating network. The 9-1-1 networks that receive calls from originating networks are not operated by Rogers. Rather, they are operated by the three large Canadian Incumbent Local Exchange Carriers ("ILECs"). They were unaffected by the outage.

(iii) whether the outage impacted broadcasting services and by extension the ability to issue public alerts via Rogers' broadcasting operations;

The Rogers network outage disabled IP connectivity between the National Alert Aggregation and Dissemination ("NAAD") system and the Rogers TV and Radio stations, removing the ability to issue BI public alerts.

Therefore, the vast majority of Rogers' over-the-air ("OTA") TV and Radio stations, were unable to receive data from the NAAD, and consequently did not issue alerts during the outage period. [redacted] That means City TV/OMNI Calgary, Lethbridge, Red Deer, Edmonton, Winnipeg, and Vancouver all had Emergency Alert System ("EAS") service available to them. To mitigate any future impact of this nature, Rogers Media is in the process of [redacted]

(iv) when and how were the operator of the National Alert Aggregation and Dissemination NAAD system, alert issuers and users notified that alerts could not be received on devices connected to the Rogers Network;

The only emergency alerts issued on July 8th were in Saskatchewan. Pelmorex reached out to Rogers Regulatory, by email, initially at 9:25am EDT and also minutes after the "Dangerous Person Alert" was issued at 9:40am EDT. Pelmorex was already aware of the Rogers network outage and asked if the alert in question was received in the field. We responded by email at 9:58am EDT, confirming that our BMC received the alert. At that moment however, we did not know whether the alert was broadcasted properly in the field.

Pelmorex sent their first email at 10:57am EDT to the entire Pelmorex Alerting Governance Council (which include, for example, all provincial governments as well as Public Safety Canada) to advise alert issuers of the Rogers outage.

At 11:19am EDT, an email from Rogers was sent to CRTC Staff and Pelmorex advising them of the national outage and cautioned that any agency attempting to broadcast emergency alerts to Rogers' customers over the Rogers networks would be unsuccessful. Pelmorex sent an update to the Alerting Governance Council (stating that the outage is continuing and that Pelmorex will issue updates as they happen) at 12:06pm EDT. Pelmorex issued further updates at 5:16pm EDT (outage is ongoing). Rogers contacted Pelmorex the following day and Pelmorex sent the last update at 4:07pm EDT on July 9th (network has been restored).

(v) whether customers were advised on how they could get alerts for their area during the outage;

Rogers' customers were not advised on how they could get alerts for their area during the outage. However, alternate last mile distributors ("LMDs") automatically distribute all alerts that are sent to them by the NAAD (see Rogers(CRTC)11July2022-2.vii below).

(vi) how were the Emergency alerts processed during the outage and were devices connected to Rogers' network able to receive alerts from other providers during the outage;

As stated above, Rogers WPAS BMC platform was operable to receive alerts from Pelmorex, but alerts could not be delivered to any wireless devices across Rogers' coverage areas during the outage. Devices connected to Rogers' Radio Access Network ("RAN") were not able to receive alerts from other Wireless Service Providers ("WSPs") during the outage. As explained in Rogers(CRTC)11July2022-2.x below, there were 4 alerts and associated updates (limited to the Province of Saskatchewan) received but not delivered to wireless devices in Rogers' coverage area.

(vii) what measures could be put in place to maintain emergency alerting capabilities during a Rogers' network outage;

In the event of a wireless network outage, emergency roaming agreements between Canadians WSPs may be able to enable wireless customers to roam onto peer wireless network(s) to receive emergency alerts and be provided with other important services such as 9-1-1. As mentioned above, it is essential that one network's outage does not impede another network's ability to continue service. Rogers, Bell and TELUS are presently assessing these potential options and will report further findings and potential solutions per the creation of the Memorandum of Understanding that will be delivered in September 2022 to the Minister of ISED by CSTAC.

Lastly, LMDs across Canada transmit alerts issued by the NAAD system. They include media such as OTA AM and FM radio and TV, electronic highway signs, and lottery terminals.

(viii) how Rogers prioritized the restoration of alerting capabilities on its network;

The only way to fully restore our alerting capabilities was to bring back on-line our IP core network. That was our absolute priority on July 8th. As a standard practice, Rogers always prioritizes the restoration of 9-1-1 and alerting capabilities on our networks.

The ability to deliver alerts to Rogers' wireless devices through the WPAS BMC platform was restored at the time of network restoration (late on July 8th). The same is true for our broadcasting systems (TV and radio). The next alert issued from the NAAD on July 9th at 3:25PM CST was successfully broadcasted upon receipt.

(ix) number of 9-1-1 calls made that could not be completed as a result of the service interruption, broken down by province and platform;

Based on available data, the number of wireless 9-1-1 calls made that could not be completed as a result of the service outage is [redacted] However, as discussed in Rogers(CRTC)11July2022-2.i above, some [redacted] calls were completed on Rogers' wireless network, [redacted] an average day's number of calls.

On an average day, Rogers wireless customers place [redacted] 9-1-1 calls, of which [redacted] are successful and [redacted] are unsuccessful. Potential event types that could result in an unsuccessful call to a PSAP include:

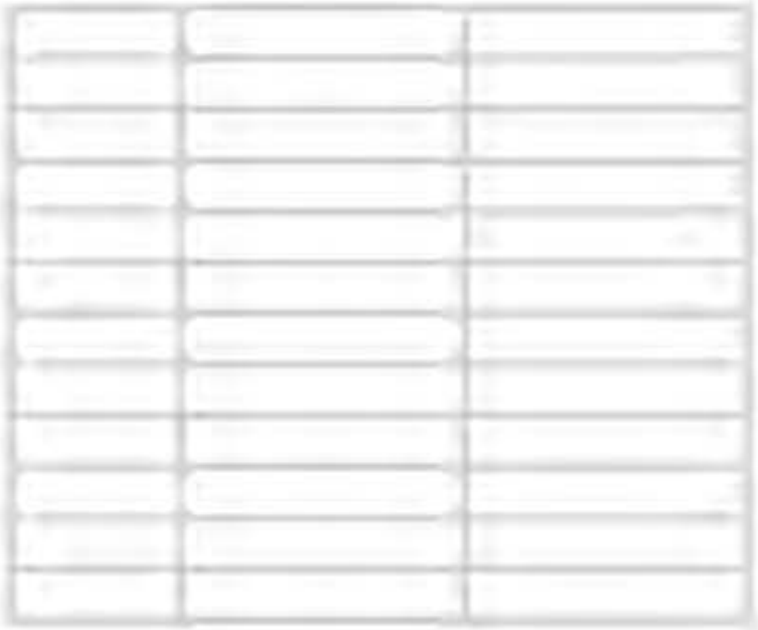
i. Manual Disconnect (a common example is a pocket dial)
ii. User Equipment ("UE") phone disconnection
iii. UE loses coverage
iv. UE runs out of battery

In our experience, it is not uncommon for customers to place additional calls to 9-1-1 to test their phone or request outage related information during an outage. Due to this behavior, some Emergency Services (such as London Police, Hamilton Police, and Ottawa Police) proactively tweeted asking Canadians not to dial 9-1-1 to test their phone or request information regarding the outage. Additionally, increased call volume could have occurred due to Rogers wireless customers having unsuccessful 9-1-1 calls and redialing 9-1-1 to attempt a successful call completion.

[redacted]

[3] A 30-second call duration was selected to identify successfully completed calls to a PSAP during the outage (i.e. [redacted] calls in total). This was to take into consideration the instability of the core network, which was impacting call completion and/or stability. Below that 30-second threshold, we consider that these were "Unsuccessful Calls".

As requested by the Commission, the table below presents the Rogers wireless 9-1-1 calls made that could not be completed, per province:



With respect to wireline 9-1-1 calls, no statistics are generated for calls that could not be completed.

(x) number of public alerts sent that did not reach Rogers' customers, broken down by province;

Only four (4) alerts were received on Rogers WPAS BMC platform on July 8th. All alerts were in the Province of Saskatchewan. No other alert was issued in Canada on that day:

1. WPAS ID 957: 7:40AM CST: Saskatchewan RCMP – Civil Emergency (Dangerous Person)
2. WPAS ID 960: 4:05PM CST: Environment Canada – Tornado (Warning)
3. WPAS ID 964: 4:19PM CST: Environment Canada – Tornado (Warning)
4. WPAS ID 982: 5:31PM CST: Environment Canada – Tornado (Warning)

(xi) how were 9-1-1 calls processed during the outage and whether they were able to be processed by other wireless networks within the same coverage area;

As seen in Rogers(CRTC)11July2022-2.i above, Rogers was able to route thousands of 9-1-1 calls on July 8th. Rogers' wireless network worked intermittently during that day as we were trying to restore our IP core network, varying region by region.

The [redacted] successful 9-1-1 calls from Rogers wireless customers to the PSAPs were processed on Rogers' wireless network when our network was available. The connection state of the UE to Rogers wireless network, and the stability of our network, determined the ability of Rogers wireless customers to have their 9-1-1 calls processed by other wireless networks within the same coverage area.

Bell and TELUS confirmed to us that some of our customers were able to connect to their wireless networks in order to place 9-1-1 calls. Bell reported [redacted] completed 9-1-1 calls and TELUS [redacted]. As such, Rogers believes that approximately [redacted] Rogers customers successfully completed 9-1-1 calls on July 8th.

(xii) whether other measures could have been taken to re-establish 9-1-1 services sooner;

The only way to fully restore the 9-1-1 service capabilities was to bring back on-line our IP core network. As mentioned before, that was our absolute priority on July 8th. As a standard practice, Rogers always prioritizes the restoration of 9-1-1 and alerting capabilities on our networks.

That said, many Rogers' wireless customers were able to connect to our network on July 8th in order to place 9-1-1 calls. See Rogers(CRTC)11July2022-2.i above for more details.

Rogers, Bell and TELUS are presently assessing potential options and will report further findings and potential solutions per the creation of the Memorandum of Understanding that will be delivered in September 2022 to the Minister of ISED by CSTAC.

No other measures would have helped restore 9-1-1 service on July 8th. One possible option that was explored by Rogers was to shut down our RAN. Normally, if a customer's device cannot connect to their own carrier's RAN, they will automatically connect to the strongest signal available, even from another carrier, for the purpose of making a 9-1-1 call. However, since Rogers' RAN remained in service on July 8th, many Rogers customers phones did not attempt to connect to another network.

Turning off the RAN was not available to Rogers on July 8th. Since our IP core was disabled, we were not able to turn off our RAN (i.e. we could have had instability issues). It would have required visits to some [redacted] Additionally, restoring the RAN would have taken several hours to complete after the core network had been restored, further extending the outage. While considered many times during the day, shutting down the RAN was simply not a solution. The best and fastest way to restore 9-1-1 was to restore the network itself.

(xiii) what alternatives are available to Rogers' customers to access 9-1-1 services during such outages;

The GSM standard for the routing of 9-1-1 calls implies that a wireless customer always has the option to remove the SIM card from their device and then to place the 9-1-1 call. The handset will register to another wireless network (the one with the strongest signal, even if there are not roaming arrangements). Phase II location information will be provided to the PSAP, but not the Caller ID (there is no callback possibility).

Further, some newer smart devices have the capability to reconnect automatically to other wireless network for 9-1-1 calls when the home network is down.

Rogers, Bell and TELUS are presently assessing potential alternatives and will report further findings and potential solutions per the creation of the Memorandum of Understanding that will be delivered in September 2022 to the Minister of ISED by CSTAC.

(xiv) details of communications related to access to emergency services over the course of the outage and whether more could have been done to explain how customers could reach 9-1-1;

At 8:39AM EDT on July 8th, the Rogers NOC first alerted the ILECs that Rogers customers were "*unable to make and receive calls nationally including 911.We are working diligently to restore services as soon as possible and will advise when restored. Please cascade this message to PSAPs accordingly*". In turn, the ILECs cascaded this information to the applicable regional PSAPs.

Many emergency service providers broadcasted to citizens on July 8th that 9-1-1 was impeded on Rogers' network with recommended measures that would assist connecting to 9-1-1, including the removal of SIM cards.

On review of our own direct efforts, there are ways to improve our communications on how customers could reach 9-1-1 in the event of an outage, including providing customers directly with more timely information stipulating 9-1-1 may not be operating properly and including resources on how they could find other ways to get connected to 9-1-1 services. Ways to improve are elaborated further in Rogers(CRTC)11July2022-2.xvi below.

(xv) details of communications to Public Safety Answering Points (PSAPs) and 9-1-1 governing authorities during the outage;

As per CRTC-approved procedures, Rogers formally communicated the service outage to the ILECs on July 8th and July 9th. The ILECs are then responsible to communicate this information to all PSAPs in Canada.

In 2017, the Commission released Telecom Decision 2017-387, establishing Canada's 9-1-1 Service Outage Notification Process created within CISC. 9-1-1 is an extremely important service that Canadians rely on in times of need when seeking emergency assistance. Rogers believes such processes are key and very important so that 9-1-1 stakeholders are aware of outages, their impacts, restoration timelines if known, and the public awareness as required.

As an Originating Network Provider ("ONP"), Rogers has the responsibility to inform our interconnecting parties an outage has occurred and to provide updates until service is restored. Updates are to be provided to the Canadian ILECs who provide 9-1-1 networks today, and of

which Rogers interconnects with: Bell, SaskTel and TELUS. In turn, the outage in question would be communicated from the ILEC to their interconnected PSAPs.

Provided in the table below is a summary of the correspondence from the Rogers NOC to the ILECs advising of the outage, updates along with resolution. The first notice was sent at 8:39 AM. In the midst of the outage, the Rogers NOC was only able to provide an update on July 8th at 5:01PM EDT. With the current CRTC process, it is recommended that hourly updates be provided by the ONPs to the ILECs. But given the network-wide impacts experienced, all support teams where focused with the immediate goal of restoring networks as quickly as possible

Communications from Rogers that were formally sent to ILECs for 9-1-1:

Notifications	Subject	Date and Time
Rogers NOC to all ILECs	National - Outage	8 July 2022 8:39AM EDT
Rogers NOC to all ILECs	Update	8 July 2022 5:01PM EDT
Rogers NOC to all ILECs	National - Restored	9 July 2022 10:51AM EDT

(xvi) Rogers' plan to enhance communications to its customers, 9-1-1 network providers, emergency management officials, PSAPs, 9-1-1 governing authorities and first responders in relation to access to 9-1-1 during a network outage;

To improve our communications with customers to provide more clarity in relation to accessing 9-1-1 during a network outage, Rogers will:

- Enhance communications and improve best practices for informing ILECs/PSAPs in the event of a network outage impacting 9-1-1;
- Use available channels (i.e. social media, IVR, chat auto-responses, rogers.com, fido.ca, public service announcements, etc.) to provide a status of 9-1-1 services;
- Deliver regular communications to customers across various channels and in-store that informs them of actions they should take if they are unable to reach 9-1-1;
- Enhance the "Rogers 9-1-1 Emergency Service" webpage on rogers.com (https://www.rogers.com/customer/support/article/911-emergency-service), including instructions on how to remove a SIM card from a wireless device and then re-dialing 9-1-1 using another wireless network, information on how to get 10-digit phone numbers for emergency services, and other ways to contact 9-1-1 (i.e. Wi-Fi calling); and
- Leverage our "9-1-1 Emergency Service" webpage in communications to customers and use it as a resource to point customers to in order to provide more information on how to contact the emergency services.

In terms of enhancing communication to 9-1-1 network providers, 9-1-1 authorities and PSAPs, Rogers is of the opinion that the current process, which include updates made in CISC ESWG ESRE0098, are the most efficient processes in place. While lessons can always be learned, the outage experienced on July 8th provided unique challenges due to the impacts to multiple Rogers' platforms and networks, not something typically experienced. CISC does actively monitor the outage notification process and should continue to do so moving forward. This should always include aspects of customer awareness. Industry members will have to work together on this communication piece in order to find proper solutions.

(xvii) extent to which the network outage affected Next Generation 9-1-1 (NG 9-1-1) networks or was in any way related to Canada's transition to NG9-1-1; and,

There was no impact as Rogers is still in the onboarding and testing phases with the ILECs.

(xviii) extent to which Rogers sought or received assistance from other TSPs in addressing the impact on emergency services arising from the service interruption.

Roger sought assistance from various other TSPs during the service interruption. We contacted them very early on July 8th. Unfortunately, there was no quick solution that would have help with the provision of emergency services during the outage.

Q3.
Past Outages

Provide a list of all service outages that affected the Rogers network since 1 January 2019, which lasted four or more hours and affected 100,000 subscribers or more at the peak. For each, indicate:

(i) the relevant timelines;
(ii) the services impacted;
(iii) the cause of the outage:
(iv) the number of customers affected, broken out by province and by TSP (Rogers affiliates, wholesale customers and others) and by type of customers (residential, small business, all other businesses/enterprises);
(v) impact on federal, provincial, territorial and municipal government services;
(vi) the extent to which any critical infrastructure sectors (e.g. financial, health, transportation, energy, etc.) were affected;
(vii) the specific impact on emergency services including public alerting and 9-1-1;
(viii) what safeguards were put in place, after each outage, to prevent future outages of that nature;
(ix) the compensation provided to customers, distinguishing between residential and business customers;
(x) whether any service level agreements (SLAs) were breached between specific vendors and Rogers in relation to this outage or what caused this outage; and,
(xi) whether Rogers breached any SLAs between itself and its customers in relation to this outage.

For each identified past outage, provide a copy of any post mortem report, including lessons learned and subsequent action plan.

A.
Rogers requests that the CRTC treat certain information contained in this Response as **confidential**, pursuant to subsection 20(1)(b) of the *Access to Information Act*, and sections 38 and 39 of the *Telecommunications Act*. For competitive reasons, and also to protect our customers as well as our networks and vendors, Rogers would never publicly disclose some of the information contained in this Response other than to the Commission. Some of the information submitted contains highly sensitive information about Rogers' networks and operations. Rogers submits that any possible public interest in disclosure of the information in this Response is greatly outweighed by the specific direct harm that would flow to Rogers and to its customers.

Rogers experienced three (3) outages since January 2019 that meet the above-mentioned criteria. More detailed information for each outage can be found in the attached Appendix entitled "CONFIDENTIAL_Rogers(CRTC)11July2022-3_Appendix 1":

In summary, these 3 outages happened on:
1) July 7th, 2019
2) April 19th, 2021
3) May 21st, 2022

The first outage was caused by a 3rd party TSP [redacted]. It affected wireless voice service across the country for almost 8 hours. Some of our customers experienced intermittent issues making or receiving wireless voice calls. With respect to 9-1-1, no dropped calls were reported to our NOC. However, it was possible that some wireless customers were not able to call 9-1-1 for emergencies during the outage. We can also confirm that [redacted]. In term of specific measures and safeguards, we assessed and addressed the following items:

[redacted]

The second outage was caused by a software upgrade made by one of Rogers' vendors. It affected wireless voice service, wireless data and texting across the country for almost 22 hours. All our wireless customers were impacted, including banking, transportation, government agencies, virtual schooling, and those working from home. Our 9-1-1 service was impacted during this outage. In that specific case, we [redacted]. That permitted our wireless customers to reconnect to other wireless networks and make 9-1-1 calls.

For this wireless outage, Rogers did provide bill credits to customers who were affected (a total of [redacted]. Lastly, since [redacted] we have diligently worked with them in order to assess and implement redress measures and further safeguards going forward. We have prepared a very detailed "Root Cause Analysis" document for this major event. See the attached Appendix entitled "CONFIDENTIAL_Rogers(CRTC)11July2022-3_Appendix 2".

The third outage was caused by severe weather conditions. It affected wireless voice service, wireless data, texting and cable services in Ontario and Quebec for almost 111 hours. 9-1-1 was impacted during this outage.

With respect to questions (v) and (vi), we do not specifically track statistics at this level of detail, but given the magnitude of these three outages, it is likely that federal, provincial, territorial and municipal government services were impacted. Similarly, critical infrastructure sectors (e.g. financial, health, transportation, energy, etc.) were likely affected too.

Concerning question (ix), no compensation was given for events #1and #3. For #2, the total compensation we have recorded is [redacted]

Finally, [redacted]

*** End of Document ***

[redacted]

Q4.
Compensation for Customers

In a message from Tony Staffieri, President and CEO of Rogers, posted on the Rogers website as of 8 July 2022, Mr. Staffieri made the commitment to "make this right" for customers by proactively applying a credit to all customers impacted by the outage.

(i) Provide the details of how Rogers is planning to honor this commitment, focusing in particular on residential and small business customers but also including other parties impacted (e.g. wholesale customers and their end-customers, etc.).
(ii) Explain how Rogers determined that this level of compensation is appropriate.
(iii) Is a distinction being made between residential customers and small business customers when determining compensation?

A.
(i) As publicly announced, Rogers will be crediting all our customers the equivalent of five (5) days of service fees. This credit will be automatically applied to the customer accounts (based on their respective monthly service plan) as of August 1st, 2022. This means that all active Rogers customers will be receiving a 5-day credit for all their services (i.e. wireless, home phone, TV and Internet), including residential and small businesses.

Wholesale accounts will also receive a 5-day credit. The Rogers Wholesale team contacted our resellers and they will be crediting their end-user for 5 days.

(ii) Rogers deliberated extensively over the proper credit amount. While the outage for most customers was approximately a day, Rogers wished to demonstrate our commitment to our customers and recognize how we let them down that day. As a result, we felt that 5 days fairly compensated our customers for their frustration with the outage.

(iii) All customers will be getting 5 days of compensation. There is no distinction between residential and small business customers.

*** End of Document ***

This is **Exhibit "2"** referred to in the Affidavit of Ron McKenzie affirmed by Ron McKenzie at the City of Toronto, in the Province of Ontario, before me on October 20, 2022 in accordance with O. Reg. 431/20, Administering Oath or Declaration Remotely.

Commissioner for Taking Affidavits (or as may be)

BRADLEY VERMEERSCH

Back to all news

Opening remarks: Standing Committee on Industry and Technology (INDU) on July 25, 2022

July 25, 2022 • Articles

[Tony Staffieri, President and CEO of Rogers Communications]

Check against delivery

Good morning Chair, members of the committee.

Thank you for the invitation to be with you.

Back to all news

I'm also responsible for the specific actions we are taking, as a company, to make sure this does not happen again.

On that day, we failed to deliver on our promise to be Canada's most reliable network.

More than a marketing slogan, we know just how critical the wireless phone and internet services Rogers provides are.

Canadians need to be able to reach their families.

Businesses need to be able to accept payments.

And, most importantly, emergency calls to 911 simply have to work, ***every*** time.

To those who were impacted by our outage, I am sorry.

Today, I want to share with you how we are working to win back the trust and confidence of Canadians.

I will start with what happened and why there was a delay in restoring our service;

I'll discuss the important steps we're taking to help prevent this from happening again.

I'll conclude with some of the steps we have begun to take to make things better for our customers.

Simply put, this outage was a result of a system failure following an update in our core network.

Back to all news

To manage those returning traffic volumes, we had to physically disconnect the impacted equipment.

Throughout this process, we had one singular and overriding focus: to get our customers up and running as quickly as we possibly could.

And I understand the frustration our customers felt, not knowing when our networks would be back online.

I wanted a timeline.

But the fact is we did not have one and didn't want to provide an estimate that might turn out to be wrong.

In the conversations I've had with customers and with small and large business owners, there is one thing everyone wants to know: what Rogers is doing – today…*now* – to learn from this outage and ensure it won't happen again.

I've said we will make every investment needed to do our best to make sure that won't happen.

That investment begins with the work now underway through our Enhanced Reliability Plan.

Working with government and our competitors, we are making significant progress on a formal agreement to ensure that 911 calls can always be made – even in the event of an outage on any carrier's network.

Back to all news

When it comes to our own network, we will do our part. And then some.

To guard against a system-wide outage, we will set a higher standard by physically separating our wireless and internet networks and create an 'always on' network.

To be frank, this added layer of protection will be expensive. We estimate it will cost at least $250 million, but know it is the right thing to do.

We will also continue with our plan to invest heavily in reliability. We're spending $10 billion over the next three years to build out and strengthen our network.

This investment includes additional oversight, more testing and greater use of Artificial Intelligence to ensure upgrades we make to our network work as intended.

Finally, we are partnering with leading technology firms to do a full review of our network systems to learn from the outage and emerge stronger.

When this work is complete, we will share the key lessons with our competitors and other industry partners.

When it comes to making things better for those who were impacted by our outage, we have already extended five days of credit for every Rogers customer.

As well, we are working with our business customers to better understand the implications of the outage on their organizations.

Chair, I know that it is only through our actions, and with time, that we can restore Canadians' confidence in us.

We can and we will do better.

Back to all news

TAGS:

Our Impact
Security & Privacy
Rogers & Shaw

Investor Relations
Leadership Team
Board of Directors

News Releases
Research & Reports
Careers

Rogers.com
Terms and Conditions
Accessibility

Contact Us
Twitter

This is **Exhibit "3"** referred to in the Affidavit of Ron McKenzie affirmed by Ron McKenzie at the City of Toronto, in the Province of Ontario, before me on October 20, 2022 in accordance with O. Reg. 431/20, Administering Oath or Declaration Remotely.

Commissioner for Taking Affidavits (or as may be)

BRADLEY VERMEERSCH

Memorandum of Understanding on Telecommunications Reliability

This Memorandum of Understanding, effective as of the Effective Date, is made by and among the parties listed in Schedule D (each a "**Party**", and collectively the "**Parties**").

Now therefore the parties agree as follows:

I. Introduction

Whereas the Parties recognize a need to ensure the reliability and resiliency of communications networks that are a significant lifeline for those in need during natural disasters, network failures and other impactful emergencies;

Whereas the Government of Canada, and specifically the Minister of Innovation, Science and Industry, has recognized the importance of telecommunications quality and resiliency, and has directed the Parties to reach agreements for coordination, roaming, mutual assistance and communications during a telecommunications emergency, including wireless- and/or wireline-based emergencies;

Whereas the Federal Communications Commission of the United States of America issued a Notice of Proposed Rulemaking, released July 6, 2022 (FCC-22-50A1), in response to a recognition that mobile services are a significant lifeline for those in need during disasters and other emergencies, requiring facilities-based wireless service providers to establish procedures for (amongst other things) (a) providing reasonable roaming under disaster arrangements when technically feasible, (b) establishing mutual aid arrangements during emergencies, and (c) taking reasonable measures to improve public awareness and stakeholder communications on service and restoration status; and

Whereas the Parties, through their participation within CSTAC, have agreed to put in place similar procedures to FCC-22-50A1 regarding (i) emergency roaming, (ii) mutual assistance, and (iii) communications to the public and governmental authorities, during a telecommunications emergency or other similarly impactful disaster.

II. Definitions

1. In this MOU, the following terms, in singular or plural form according to the context, are defined as follows, and capitalized terms used but not otherwise defined have the meanings given in the Schedules:

"**Accident**" means an event that happens by chance or that is without apparent or deliberate cause and can happen during planned maintenance or normal operations.

"**Affiliate**" means any entity controlling, controlled by or under common control of a Party, as the context requires. For this definition, "control" means the: (i) direct or beneficial ownership of fifty percent (50%) or more of the entity's voting securities; or (ii) ability to elect a majority of the entity's directors.

"**Applicable Law**" means all applicable laws and regulations of any governmental authority having the force of law in Canada.

"**Bilateral Emergency Roaming Agreement**" has the meaning ascribed thereto in Section 4 of Schedule A – Emergency Roaming Protocol.

"**Confidential Information**" of a Party means any and all material and information of a Party (the "**Discloser**") or its Affiliates which has or will come into the possession or knowledge of another Party (the "**Recipient**") in connection with or as a result of entering into this MOU (including the terms of this MOU), and information concerning the Discloser's or its Affiliates'

past, present and future customers, vendors, and business. For the purposes of this definition, "information" and "material" includes know-how, data, patents, copyrights, trade secrets, processes, techniques, programmes, designs, formulae, marketing, advertising, financial, commercial, sales or programming materials, written materials, compositions, drawings, diagrams, computer programs, studies, work in progress, visual demonstrations, ideas, concepts, and other data, in oral, written, graphic, electronic, or any other form or medium whatsoever. Notwithstanding the foregoing, "Confidential Information" does not include the following information:

a. information which is in the public domain when it is received by or becomes known to the Recipient or which subsequently enters the public domain through no fault of the Recipient (but only after it enters the public domain);
b. information which is already known to the Recipient at the time of its disclosure to the Recipient by the Discloser and is not the subject of an obligation of confidence of any kind;
c. information which is received by the Recipient in good faith without an obligation of confidence of any kind from a third party who the Recipient had no reason to believe was not lawfully in possession of such information free of any obligation of confidence of any kind, but only until the Recipient subsequently comes to have reason to believe that such information was subject to an obligation of confidence of any kind when originally received;
d. information which is independently developed by the Recipient without any use of or reference to the Confidential Information of the Discloser and which such independent development can be established by evidence that would be acceptable to a court of competent jurisdiction; and

e. information which is not subject to an obligation of confidence of any kind when released, disclosed, made available or communicated by the Discloser to a third party.

"**Contact Information**" means the first and last names of the primary and secondary contacts, corresponding email addresses, mobile telephone numbers, professional titles and job functions for each Party, Governmental Authority, and ISED, as the case may be, as amended over time, including:

a. home carrier mobile phone number and alternative carrier mobile phone number (i.e. an individual's mobile phone number on an alternative carrier network in the event that the home carrier mobile phone number is unreachable);
b. home carrier email address and non-carrier email address (i.e. an individual's alternate non-carrier email address in the event the home carrier network or home carrier email address is unreachable); and
c. any other contacts and/or contact information which the Party considers relevant, e.g., additional contact names, contact information for a Party's network operations centre.

"**Contact Roster**" means the totality of the Contact Information maintained in accordance with Section 7.c. of this MOU.

"**Contributed Materials**" means all materials, information, methods, software, hardware, work, devices, documents, concepts, approaches, tools, and/or items provided or contributed by a Party under this MOU.

"**Critical Network Failure**" means an unintentional and unplanned Network outage caused by, or occurring in the context of an Impactful Emergency.

"**CRTC**" means the Canadian Radio-television and Telecommunications Commission or its successor.

"**CSTAC**" means the Canadian Security Telecommunications Advisory Committee, or its successor.

"**Discloser**" has the meaning ascribed thereto in the definition of "Confidential Information" in this Section 1.

"**Effective Date**" means September 9, 2022.

"**Existing Roaming Agreement**" has the meaning ascribed thereto in Section 4 of Schedule A – Emergency Roaming Protocol.

"**Governmental Authorities**" means the CRTC, the offices of the Minister of Emergency Preparedness or its successor, the Minister of Public Safety or its successor, the Minister of Innovation, Science and Industry or its successor, or their respective duly appointed delegates, and the appropriate Provincial or Territorial Minister within the jurisdiction(s) experiencing a Triggering Event (each a "**Governmental Authority**").

"**Impactful Emergency**" means an urgent and critical situation that seriously endangers the lives, health or safety of Canadians, including but not limited to those arising from Accidents, cyber attacks or other deliberate malicious acts, fires, floods, storms, earthquakes, emergencies arising from domestic or international security threats, or armed conflicts involving Canada or its allies.

"**Intellectual Property Rights**" means: (1) any and all proprietary rights provided under, (a) patent law, (b) copyright law, (c) trade-mark law, (d) design patent or industrial design law, (e) semi-conductor chip or mask work law, or (f) any other statutory provision or common law principle, including trade secret law, which may provide a right in either ideas, formulae, algorithms, concepts, inventions or know-how generally, or the expression or use of such ideas, formulae, algorithms, concepts, inventions or know-how;

and (2) any and all applications, registrations, licences, sub-licences, franchises, agreements or any other evidence of a right in any of the foregoing.

"**ISED**" means Innovation, Science and Economic Development Canada or its successor.

"**MOU**" means this document entitled "Memorandum of Understanding" and all schedules attached as of, or added following, the Effective Date ("**Schedules**").

"**Network**" has the meaning ascribed thereto in each Schedule as applicable.

"**Personal Information**" means information concerning an identifiable individual.

"**Programme**" has the meaning ascribed thereto in Section 2 hereof.

"**Protocols**" means one or the combination of policies, procedures, guidelines, protocols, playbooks, and/or agreements.

"**Recipient**" has the meaning ascribed thereto in the definition of "Confidential Information" in this Section 1.

"**Triggering Event**" means a Critical Network Failure subject to a Triggering Event Declaration.

"**Triggering Event Declaration**" means a notification, pursuant to Section 7.d. hereof, by a Party who is experiencing or is likely to experience a Critical Network Failure to another Party that it is activating the Emergency Roaming Protocol and/or the Mutual Assistance Protocol in respect thereof.

"**Triggering Event Duration**" means the period of time between the Triggering Event Start Point and the Triggering Event End Point.

"**Triggering Event End Point**" means the earlier of (A) notification, pursuant to Section 7.e. hereof, by the Party who issued the Triggering Event Declaration to the Party who is providing Emergency Roaming and/or the Mutual Assistance that it is revoking the Triggering Event Declaration, and (B) the resolution of the Critical Network Failure.

"**Triggering Event Start Point**" means the issuance of a Triggering Event Declaration.

III. Purpose

2. The purpose of this MOU is to establish Protocols for (i) emergency roaming between the Parties, as applicable, (ii) mutual assistance of the Parties, as required, and (iii) communication to the public and Governmental Authorities, during a Critical Network Failure resulting from an Impactful Emergency (the "**Programme**").

IV. Agreement of the parties

3. **Term**: This MOU, including any amendments made to it going forward pursuant to the amendment process set out in Section 4 hereof, comes into force as of the Effective Date (or, in the case of any amendments, as of the date that such amendments are agreed to by all the Parties) and ends 5 years after the Effective Date (the "**MOU Initial Term**") subject to Section 4 hereof. Upon the expiry of the MOU Initial Term, the MOU will be automatically extended for successive one year renewal terms until terminated by all Parties with at least 30 days' written notice prior to the end of any renewal term. The MOU Initial Term and any renewal terms are collectively referred to as the "**MOU Term**".

4. **Amendments**:

a. This MOU may be amended or supplemented, including to add new parties to this MOU, by mutual written agreement executed by each Party.
b. Any Party may, at any time during the Term, propose an amendment or amendments to the MOU and its Protocols by notice to the other Parties in writing, whereupon the Parties agree to meet within 90 days to consider any such proposals. Notice of proposed amendments should clearly specify the section or sections of the MOU or any Protocol that a Party seeks to amend (if any), the specific amendment, amendments or addition proposed, and the rationale for each proposed amendment or addition, in order that the Parties may fully consider and respond to the proposal.

5. **Termination**: Subject at all times to Section 16 and notwithstanding Section 3, a Party may terminate its participation in this MOU during the MOU Term, with no cost, liability or future obligation on the part of such Party, forthwith upon 6 months' prior written notice to each other Party, provided, however, that no termination may occur during a Triggering Event Duration. For certainty, a Party's termination of its participation under this MOU will not automatically result in termination of any Bilateral Emergency Roaming Agreements or other agreements that such Party has entered into in accordance with the terms and conditions of this MOU. Any such agreements may only be terminated by such Party in accordance with their respective terms.

6. **Programme Implementation**: During the MOU Term, the Parties will operationalize the following Protocols based upon the terms and conditions of this MOU:

a. Emergency Roaming Protocol as specified in Schedule A of this MOU;
b. Mutual Assistance Protocol as specified in Schedule B of this MOU; and

PUBLIC

c. Emergency Network Outage Communications Protocol as specified in Schedule C of this MOU.

7. **Communications:**

a. The Parties will use the Traffic Light Protocol ("**TLP**") definitions below to facilitate the sharing of information under the Programme.

Definition	**Rules of Disclosure**	**Description**
TLP:RED	not for further disclosure, restricted to recipients only	recipients may not share information with any persons outside of the specific exchange, meeting, or conversation in which it was originally disclosed
TLP:AMBER	limited disclosure allowed, restricted to within Party	recipients may only share information with members of their own Party who need to know the information
TLP:GREEN	limited disclosure, restricted to within all Parties	recipients may share information with members of their own Party or other Parties but not via publicly accessible channels
TLP:WHITE	disclosure not limited	Recipient may share information without restriction

b. Each Party will designate one or more individuals as "Senders" and "Addressees" of the information to be transmitted under this

Programme, and supply the list of its Senders and Addressees to the other Parties. A Party's Sender will obtain confirmation that the transmission by that Sender of information to the other Party was successful.

c. Contact Roster:
    i. Each Party shall be required to maintain (a) an up-to-date list of its Contact Information, and (b) a list of the most recently provided Contact Information from the other Parties, Governmental Authorities and ISED (to the extent provided).
    ii. Each Party shall share its Contact Information with CSTAC every 6 months during the MOU Term, or upon making a change to its Contact List, for the purpose of CSTAC being able to maintain an up to date Contact Roster.
    iii. Each Party shall, every 6 months during the MOU Term or as otherwise offered by CSTAC, participate in CSTAC testing to confirm the accuracy of the Contact Roster.
d. Triggering Event Declaration: A Triggering Event Declaration is not initiated by a Party until such Party reaches, by phone, one or more of the contacts on the Contact Roster of the Party from whom Emergency Roaming and/or Mutual Assistance is requested. As soon as practicable following receipt of such phone call, the Party from whom Emergency Roaming and/or Mutual Assistance was requested shall send an email to the Party who initiated the phone call confirming: (A) receipt of the phone call initiating a Triggering Event Declaration, (B) the date and time of the phone call, (C) whether Emergency Roaming or Mutual Assistance or both was requested.
e. Notice of Triggering Event Revocation. A Party who initiated a Triggering Event Declaration may revoke the Triggering Event Declaration by sending an email to the contacts on the Contact Roster of the Party from whom Emergency Roaming and/or Mutual Assistance was requested.

8. **Intellectual Property Rights**: In the event that a Party ("**Licensor**") provides any Contributed Materials to another Party ("**Licensee**") for use in connection with the Programme, then, subject to the terms and conditions of this MOU and, where applicable, the terms and conditions of Licensor's suppliers or licensors, Licensor hereby grants to Licensee a non-exclusive, non-sublicensable, non-transferable, royalty-free license to use the Contributed Materials solely for the purpose of the performance of Licensee's obligations or exercise of Licensee's rights under this MOU in connection with the Programme. Title to, ownership of, and all Intellectual Property Rights in, any Contributed Materials provided hereunder shall be and remain with the Licensor or its suppliers or licensors, and no other Party will acquire any Intellectual Property Rights therein other than the licence explicitly granted herein. Licensee acknowledges and agrees that all Contributed Materials are provided on an as-is basis and without any representations or warranties from Licensor of any kind, whether express or implied.

9. **No Monetization of Information Received under this MOU**: Without limiting any other provision of this MOU, under no circumstance may a Party receiving information pursuant to this MOU (i) directly or indirectly monetize, or (ii) consent to the monetization of that information in any way including by selling or licensing said information, without the express written consent of the other Parties.

10. **Exclusivity**: Notwithstanding any other provision of this MOU, the Parties acknowledge and agree that this MOU in no way limits or prohibits a Party from entering into any discussion, agreement memorandum or other arrangement with any other entity, concerning the subject matter hereof.

11. **Costs**: Except as specifically stated in this MOU or an applicable Bilateral Emergency Roaming Agreement, each Party shall pay its own costs and expenses related to the negotiation, participation and implementation of this

MOU.

12. **Warranties**: The Parties acknowledge and agree that no Party is providing a warranty of integrity or accuracy of any information provided pursuant to this MOU, nor is any Party providing any representation, warranties, conditions or guarantees regarding the actions or activities contemplated by or under this MOU (implied or statutory).

13. **Liability**:

a. Each Party's participation in this MOU and its use of the information transferred under this MOU is at its own risk.
b. Except (i) as specifically stated in an applicable Bilateral Emergency Roaming Agreement, (ii) for a Party's indemnity obligations set forth in Schedule A and Schedule B, (iii) for a Party's breach of Section 14 (Confidentiality), (iv) for a Party's infringement or misappropriation of another Party's Intellectual Property Rights, (v) for damage to a Party's tangible property caused by another Party's negligence or wilful misconduct, (vi) for bodily injury or death to any person caused by a Party's negligence or wilful misconduct, (vii) for damages caused by a Party's gross negligence or wilful misconduct, and (viii) for a Party's obligation to pay any fees or costs or expenses hereunder, no Party shall be liable to any other Party for any direct damages, costs, losses or expenses, nor commence or otherwise maintain against the other Party any claim, action, suit or other proceeding, whether in contract, tort or otherwise, resulting from or arising in connection with any claim arising under or in connection with this MOU.
c. Except (i) as specifically stated in an applicable Bilateral Emergency Roaming Agreement, (ii) for a Party's indemnity obligations set forth in Schedule A and Schedule B, (iii) for a Party's breach of Section 14 (Confidentiality), and (iv) for damages caused by a Party's gross negligence or wilful misconduct, no Party shall be liable to any other

Party for any indirect, incidental, special or consequential damages whatsoever arising under or in connection with this MOU, or the following damages whether characterized as direct, indirect, incidental, special or consequential damages: lost profits, anticipated or lost revenue, loss of data, loss of business opportunities, loss of use of any information system, failure to realize expected savings or any other commercial or economic loss, whether arising in negligence, tort, statute, equity, contract, common law, or any other cause of action or legal theory, and whether pursuant to common law, equity, or statute, even if a Party has been advised of the possibility of such damages.

d. No Party shall be obligated to comply with this MOU, perform any act or omission, or otherwise conduct itself, in a manner that is contrary to Applicable Laws.
e. The Parties agree that, to the extent a Responding Party acting in good faith and in accordance with this MOU and any Bilateral Emergency Roaming Agreement engages in activities described in Schedules A, B or C hereto, then, the Parties agree not to commence a Part 1 Application or similar complaint under the CRTC Rules of Procedure against such Responding Party in respect of its conduct in the context of a Triggering Event, including without limitation, a complaint pursuant to section 27(2) of the Telecommunications Act.

14. **Confidentiality:**

a. From time to time, the Confidential Information of a Discloser or its Affiliates may come into the possession or knowledge of a Recipient. The Recipient shall:
    i. protect and safeguard the confidentiality of the Discloser's Confidential Information with at least the same degree of care as the Recipient would protect its own Confidential Information of a

similar nature, and in no event with less than a reasonable degree of care;

ii. not use the Discloser's Confidential Information, or permit it to be accessed or used, for any purpose other than to exercise its rights or perform its obligations under this MOU;

iii. not disclose the Discloser's Confidential Information to any third party, except to: (1) the Recipient's representatives who need to know the Confidential Information for the Recipient to exercise its rights or perform its obligations pursuant to this MOU and who are bound to protect the received Confidential Information from unauthorized use or disclosure under written confidentiality obligations no less protective of Discloser than those contained in this MOU and (2) other persons for whom the Discloser has provided its written consent. For clarity, the Recipient shall be responsible for any breach of this MOU caused by any of its representatives; and

iv. notwithstanding the foregoing, the Parties shall notify and consult with each other as soon as possible in the event that it is required by law to disclose Confidential Information as defined in this MOU.

b. In addition to the obligations set forth above in this Section 14, the Parties shall hold any Personal Information secure in accordance with industry practices and shall comply with all Applicable Laws relating to the protection and privacy of the Personal Information, including the *Personal Information Protection and Electronic Documents Act* (Canada) ("**PIPEDA**"). A Party shall not disclose any Personal Information which it accesses or receives through its interactions with another Party to any third party whatsoever, except as specifically authorized under PIPEDA or this MOU. The Parties shall not use any Personal Information for any marketing, preference tracking or other purposes not directly related to its performance of its obligations pursuant to this MOU.

c. Each Party agrees and covenants that neither it nor any of its respective officers, directors or agents, will at any time make, publish or communicate to any third party or in any public forum any defamatory, libelous or slanderous remarks, comments or statements concerning any other Party's performance under this MOU, or that of any of its officers, employees, directors, and other associated third parties.
d. The Parties will not use the existence of this MOU or any of the provisions herein for marketing or promotional purposes.

15. **Data Retention and Destruction**:

a. The Parties understand they are expected to not retain Confidential Information for longer than is reasonably needed to fulfil the purpose for which the Confidential Information was shared, or as otherwise required by Applicable Laws, whichever is longer.
b. Upon the termination or expiration of this MOU or when the Confidential Information is no longer needed for the purpose for which it was disclosed, whichever occurs first, a Party will promptly return to the applicable other Party or securely destroy all Confidential Information of the other Party and any Personal Information which is then in its possession or control (except copies made for archival or back-up purposes, which the Party will destroy no later than one year following the date of termination or expiration or when the Confidential Information is no longer needed, as applicable). Any such destruction shall render the applicable Confidential Information or Personal Information permanently unreadable and unrecoverable and the Recipient Party shall provide the Disclosing Party with prompt written certification of such destruction.

16. **Survival**: In the event of expiration or termination of this MOU, Sections 1, 8, 13, 14, 15, 16, 18, 20, and 21, and all such other provisions to give effect thereto, shall survive such expiration or termination indefinitely.

17. **Authority**: Each Party confirms that its representative signing this MOU has the authority to do so.

18. **Governing Law and Jurisdiction**: This MOU shall be governed by, and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein. Except as provided in Section 20 below, each Party irrevocably attorns to the exclusive jurisdiction of the courts of Ontario for any dispute, controversy, or claim (including any questions of this MOU's existence, validity or termination) arising in connection with this MOU.

19. **Notices**: Any legal notice that must be given or made under this MOU or which a Party wishes to give to another Party, or the other Parties, must be given in writing and is properly transmitted if it is delivered by courier or email to the corresponding address(es) listed in Schedule E. Any notice sent in accordance with the foregoing shall be deemed to have been received by its addressee upon delivery.

20. **Dispute Resolution**:

a. If any dispute, issue disagreement, or question (in this Section called a "**Dispute**") arises during the MOU Term between two or more Parties concerning this MOU or any part hereof, the Parties shall in good faith attempt to resolve such Dispute promptly and in an amicable manner under the following informal Dispute resolution procedure.
    i. If a Dispute arises which is not resolved, each Party involved in the Dispute shall designate a Vice President or higher (the "**Executive Managers**") to attempt to resolve the Dispute.
    ii. The Executive Managers shall meet as promptly as possible.
    iii. If the Executive Managers cannot resolve the Dispute within 20 business days after being notified of a Dispute, the Dispute shall be referred to each Party's CEO, and the applicable CEOs shall meet

within 20 business days after being notified of a Dispute to attempt to resolve the Dispute.

iv. Notwithstanding the above, should a Party in a Dispute consider (acting in good faith) the Dispute to be of such an urgent nature as to require expedient resolution, the Parties shall each designate an Executive Manager to meet to resolve the Dispute within two (2) hours after being notified, or otherwise as promptly as possible, and if the Executive Managers cannot resolve the Dispute within 4 hours after being notified of a Dispute, the Dispute shall be referred to each Party's CEO, and the applicable CEOs or their designates shall meet within 6 hours after being notified of a Dispute, or otherwise as promptly as possible, to attempt to resolve the Dispute.

b. If the Parties are unable to settle a Dispute after complying with Section 20(a) hereof, a Party may, on written notice to the other Parties involved in the Dispute (a "**Notice of Arbitration**"), require that such unresolved Dispute be resolved by arbitration in accordance with the Ontario Arbitration Act, 1991 (Ontario) (the "**Arbitration Act**") and subject to Section 20(c) below.

c. The following provisions shall govern each Dispute referred to arbitration under Section 20(b) hereof.

i. Such arbitration shall be held in Toronto, Ontario, (with accommodations for Parties to attend via videoconference).

ii. The procedures for the resolution of Disputes set out in this Section 20 do not preclude recourse to the courts for urgent interim, injunctive or interlocutory relief.

iii. The arbitration shall be conducted in English or in English and French when one or more of the Parties involved in the arbitration request it.

iv. The arbitration will take place before a panel of one arbitrator, selected by the Parties involved in the Dispute. If the Parties are

unable to agree on a single arbitrator, then a Party may apply to the Ontario Superior Court of Justice for the appointment of an arbitrator in accordance with the Arbitration Act. The arbitrator appointed will be a retired judge or a lawyer with extensive arbitration qualifications and experience.

v. Any award or decision made by the arbitrator appointed is final and binding upon the parties to this MOU with a right of appeal on questions of law alone. Any award or decision of the arbitrator may be enforced in the manner provided for by the Arbitration Act.

vi. Each Party will be responsible for its own legal costs in connection with the arbitration. The arbitrator's fees and disbursements will be shared equally by the Parties involved in the arbitration, unless the arbitrator determines that a specific Party(ies) prevailed, in which case the arbitrator's fees and disbursements will be shared equally by the non-prevailing Party(ies).

vii. Subject to Applicable Law, the Parties agree to keep the arbitration procedures, hearings, documents and award strictly confidential and will not, unless required by law, voluntarily disclose any information concerning the fact or outcome of any arbitration, with the sole exception of legal counsel, accountants and financial advisors providing that they first agree to keep such information strictly confidential.

21. **General**:

a. This MOU shall enure to the benefit of and be binding upon the Parties and their respective heirs, executors, administrators, legal personal representatives, successors and assigns.

b. In this MOU words importing the singular number only shall include the plural and vice versa and words importing any gender shall include all other genders and words importing persons shall include individuals,

partnerships, associations, trusts, unincorporated organisations and corporations and vice versa. The term "including" means "including, without limitation".

c. Unless otherwise specified, any reference herein to a "day" shall mean a calendar day.

d. This MOU may be executed in several counterparts or using separate signature pages, and each such executed counterpart and each counterpart to which such executed signature pages are attached shall be deemed to be an original, and such counterparts together shall constitute one and the same instrument. This MOU shall not become a valid and binding agreement between the Parties unless and until each Party has duly executed and delivered to the other Parties one copy of this MOU.

e. The rights and remedies of the Parties hereunder are cumulative and are in addition to, and not in substitution for, any other rights and remedies available at law or in equity or otherwise. No single or partial exercise by a Party of any right or remedy precludes or otherwise affects the exercise of any other right or remedy to which that Party may be entitled.

f. If any provision of this MOU is held to be invalid or unenforceable in whole or in part, such invalidity or unenforceability shall attach only to such provision or part thereof and the remaining part of such provision and all other provisions hereof shall continue in full force and effect.

g. No amendment of any provision of this MOU shall be effective unless such amendment is in writing signed by all Parties and stating specifically that it is intended to modify this MOU. No waiver of any breach of or non-compliance with any provision of this MOU shall be effective or binding unless made in writing and signed by the Party purporting to give the same and, unless otherwise specified in the written waiver, shall be limited to the specific breach waived. No waiver

shall be inferred from or implied by any failure to act or delay in acting by a Party in respect of any default, breach, non-observance or by anything done or omitted to be done by another Party.

h. This MOU, together with any Schedules attached to this MOU and any agreements and documents to be delivered pursuant to the terms of this MOU, constitutes the entire agreement between the Parties pertaining to the subject matter of this MOU and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, of any of the Parties in respect of the subject matter hereof. There are no conditions, representations, warranties or other agreements between the Parties in connection with the subject matter of this MOU, whether oral or written, express or implied, statutory or otherwise, except as specifically set out in this MOU. Notwithstanding anything to the contrary in the MOU, the Parties acknowledge and agree that in no event will the MOU be deemed to amend, modify or supersede the terms and condition of any Existing Roaming Agreement.
i. A Party may freely assign all or any part of this MOU to an Affiliate upon the provision of prior written notice to the other Parties provided that such Party remains responsible and liable for the acts and omissions of such Affiliate. Except as set forth in the immediately preceding sentence, no right or interest in this MOU shall be assigned or subcontracted by a Party without the prior written consent of the other Parties and no delegation of the performance of any obligations owed by a Party to any other Party shall be made without the consent of the other Parties, in each case such consent not to be unreasonably delayed or denied.
j. The original English version of this MOU has been translated into French. In the event of inconsistency or discrepancy between the English version and the French version of this MOU, the English language version shall prevail.

[Signature pages follow.]

IN WITNESS WHEREOF, the Parties hereto have executed this MOU as of the Effective Date.

BELL CANADA

Name: Mirko Bibic

Title: President and Chief Executive Officer

Date: September 6, 2022

[Signature pages continue.]

BRAGG COMMUNICATIONS INC.

Name: Signatory: Lee Brag

Title: Executive Vice Chair

Date: September 1, 2022

[Signature pages continue.]

COGECO COMMUNICATIONS INC.

Name: Philippe Jetté

Title: President and Chief Executive Officer

Date: September 6, 2022

[Signature pages continue.]

ROGERS COMMUNICATIONS CANADA INC.

Name: Anthony Staffieri

Title: President and Chief Executive Officer

Date: September 1, 2022

PUBLIC

[Signature pages continue.]

SASKATCHEWAN TELECOMMUNICATIONS

Name: Doug Burnett

Title: President and Chief Executive Officer

Date: September 2, 2022

[Signature pages continue.]

SHAW COMMUNICATIONS INC.

Name: Brad Shaw

Title: Executive Chair and Chief Executive Officer

Date: September 6, 2022

FREEDOM MOBILE INC.

Name: Brad Shaw

Title: Executive Chair and Chief Executive Officer

Date: September 6, 2022

[Signature pages continue.]

TBAYTEL

Name: Daniel Topatigh

Title: President and Chief Executive Officer

Date: September 6, 2022

[Signature pages continue.]

TELESAT CANADA

Name: Christopher DiFrancesco,

Title: VP, General Counsel and Secretary

Date: September 1, 2022

[Signature pages continue.]

TELUS COMMUNICATIONS INC.

Name: Darren Entwistle

Title: President and Chief Executive Officer

Date: September 2, 2022

[Signature pages continue.]

VIDEOTRON LTD.

Names: Pierre Karl Péladeau and Sophie Riendeau

Titles: President and Corporate Secretary

Date: September 6, 2022

[Signature pages continue.]

XPLORNET COMMUNICATIONS INC.

Name: Allison Lenehan

Title: President and Chief Executive Officer

Date: September 2, 2022

[Signature pages continue.]

ZAYO CANADA INC.

Name: Michael Strople

Title: Managing Director Zayo Canada

Date: September 6, 2022

[Signature pages end.]

Schedule A

Emergency Roaming Protocol

Purpose:

1. This Emergency Roaming Protocol applies when one or more Parties provides Emergency Roaming to another Party when the latter Party is experiencing a Triggering Event.

Definitions:

2. Unless specifically defined hereunder, capitalized terms shall have the meanings set out in the body of the MOU or Schedule B or Schedule C, as the case may be. In this Emergency Roaming Protocol, the following terms, in singular or plural form according to the context, are defined as follows:

a. "**9-1-1 Wireless Access**" means voice access to available 9-1-1 networks via a wireless handset.
b. "**Emergency Roaming**" means as stated in Section 3 of this Emergency Roaming Protocol.
c. "**Emergency Roaming Protocol**" means this Schedule A – Emergency Roaming Protocol to the MOU, as it may be amended over time.
d. **"Network"** means a Party's wireless network including, as the case may be, the access network, network core, backhaul, transport connectivity and the infrastructure, in whole or in part.
e. "**Receiving Party**" means a Party that receives Emergency Roaming, under this Emergency Roaming Protocol.
f. "**Responding Party**" means a Party that provides Emergency Roaming, under this Emergency Roaming Protocol.

Forms of Emergency Roaming

3. Consistent with the principles herein, Emergency Roaming consists of the provision of domestic voice, text and data roaming services on an emergency basis when technically feasible during a Triggering Event, in whole or in part, by a Responding Party to a Receiving Party during the entirety, or part of, a Triggering Event. For clarity, Emergency Roaming includes the provision of 9-1-1 Wireless Access and excludes the provision of Mutual Assistance (as described in Schedule B to this MOU), Emergency Network Outage Communications Protocol (as described in Schedule C to this MOU) and other forms of assistance not expressly provided for under this Emergency Roaming Protocol.

Bilateral Emergency Roaming Agreements

4. Within 9 months of the Effective Date, the Parties will enter into confidential reciprocal bilateral Emergency Roaming agreements, or one or more confidential reciprocal multilateral Emergency Roaming agreements, with those Parties with whom they have overlapping Networks to address Emergency Roaming, (collectively the "**Bilateral Emergency Roaming Agreements**") in order to effect the provision of available Emergency Roaming pursuant to this Emergency Roaming Protocol. Nothing in this MOU shall prevent two Parties that have an existing bilateral commercial wholesale roaming agreement ("**Existing Roaming Agreement**") and overlapping Networks, from agreeing in writing (email being sufficient) to amend such Existing Roaming Agreement to address Emergency Roaming. If two Parties agree to use an Existing Roaming Agreement to address Emergency Roaming, the applicable Parties will enter into a written amendment to the Existing Roaming Agreement to address Emergency Roaming within 9 months of the Effective Date. For clarity, if the applicable Parties so agree in writing, and for the purposes of this MOU and the terms and conditions set forth herein, then their amended Existing Roaming

Agreement, insofar as it applies to the provision of available Emergency Roaming, will be considered a Bilateral Emergency Roaming Agreement hereunder and the terms and conditions set forth herein that apply to Bilateral Emergency Roaming Agreements, including the Principles, the Additional Terms and the Responding Party Indemnity set forth below, will apply to such amended Existing Roaming Agreement.

Principles

All Bilateral Emergency Roaming Agreements will incorporate the following principles:

5. Emergency Roaming may only be invoked by a Party in case of a Triggering Event Declaration and only after having tried, on a best efforts basis, to take all possible steps to restore services on its own Network(s). For greater certainty, a Party shall be prohibited from initiating a Triggering Event Declaration as part of that Party's response to operational Network outages that do not fall within the definition of a Critical Network Failure.
6. The provision of Emergency Roaming by a Responding Party is conditional on the Receiving Party taking all possible steps, throughout the Triggering Event Duration, to restore services on its own Network(s) on a best efforts basis.
7. The conduct of a Receiving Party and any Responding Party pursuant to this Emergency Roaming Protocol shall at all times be governed by the duty of good faith.
8. A Responding Party shall use reasonable efforts to provide Emergency Roaming to the Receiving Party in a Triggering Event for the Triggering Event Duration. However, nothing in this Emergency Roaming Protocol prevents a Party from assisting another Party outside the scope of this Emergency Roaming Protocol.
9. Where a Triggering Event Declaration is made, coincident with the Triggering Event Start Point, or as soon thereafter as reasonably practicable,

the Responding Party may request and the Receiving Party shall use reasonable efforts to provide information about the Triggering Event, including: a description of the Critical Network Failure, location(s), estimated duration, impacted Network nodes, identification of any other Parties providing Emergency Roaming and an estimate of the type and quantity of Emergency Roaming required in both number of subscribers/sessions and the amount of traffic.

10. A Receiving Party shall receive the scope, extent and quality of Emergency Roaming provided by a Responding Party, on an "as is and where is" basis. For greater certainty there is no duty hereunder upon a Responding Party to augment or supplement its existing Network capacity.

11. A Responding Party is required to provide only such reasonable scope and extent of Emergency Roaming, and only to a level that can be accommodated by its existing Network capacity and that will not, in the sole opinion of that Responding Party, materially adversely impact the services it ordinarily provides to its own end-user customers, and to do so where feasible, provided that the Responding Party has reasonably first managed its own Network needs. Without limiting the generality of the foregoing, a Responding Party may, in its sole discretion, decline to provide Emergency Roaming, implement traffic management practices, or withdraw some or all of the Emergency Roaming it had been providing, to the extent the Responding Party is (a) unable to provide, or continue providing, such Emergency Roaming, (b) experiencing a Triggering Event itself, or (c) experiencing or reasonably anticipates experiencing material service degradation due to traffic volumes, network capacity considerations, security events or other factors.

12. A Party that is experiencing a material adverse impact to its Network due to an increase in roaming traffic as a result of a Critical Network Failure of another Party/Parties, may take steps to manage its Network in advance of the other Party/Parties issuing a Triggering Event Declaration. The Party that

takes steps to manage its Network will provide details of such Network management to the affected Party/Parties within 24 hours of implementing such Network management.

13. In the case where a Triggering Event is followed by one or more Triggering Events, the Parties agree and acknowledge that each Responding Party, as the case may be, shall be required to triage and re-prioritize the scope and extent of their Emergency Roaming and may reasonably redeploy resources in accordance with the scope and severity of the various Triggering Events.

14. Unless specifically stated otherwise in this Emergency Roaming Protocol, Emergency Roaming shall be wound down and terminated as soon as possible based upon the best efforts of the affected Parties to restore service(s) to their end-user customers and upon the restoration of such services.

15. To the extent two or more Parties may experience the same Triggering Event, for example due to the same natural disaster, they shall attempt to coordinate their resources to the extent practicable and reasonable.

16. Where a Responding Party implements traffic management practices or declines to provide or withdraws, Emergency Roaming, in whole or in part, to a Receiving Party:

1. the Responding Party will provide details of the implemented traffic management practices within 24 hours of implementing such practices;
2. the Responding Party will provide advance notice of withdrawal where possible; and
3. the Receiving Party shall be entitled to request the reason(s) for the Responding Party's declining or withdrawal of Emergency Roaming, and the Responding Party shall provide such reasons in writing within 24 hours of receiving such request.

17. During a Triggering Event, a Receiving Party will take all reasonable steps to provide as much network availability as practicable to its own customers in

the impacted geographical scope of the Triggering Event ("**Emergency Roaming Area**").

18. Network considerations may require the Parties to tailor Emergency Roaming to allow or curtail different traffic types as necessary. Parties acknowledge and agree that Emergency Roaming will not provide the same type of service or quality of service as is provided as part of wholesale commercial roaming, whether under commercial agreement or under the applicable CRTC wholesale roaming tariff.

19. By requesting Emergency Roaming, the Requesting Party accepts that the type of service or quality of service provided by the Responding Party pursuant to a commercial roaming agreement or under an applicable CRTC wholesale roaming tariff, as the case may be, may be negatively impacted by the provision of Emergency Roaming.

20. When providing Emergency Roaming during a Triggering Event, the Responding Party will, to the extent feasible, prioritize the transmission of 9-1-1 Wireless Access voice traffic above all other wireless traffic on its Network.

Additional Terms

21. In addition to incorporating the above principles, the Bilateral Emergency Roaming Agreements will also contain:

a. clear definitions for determining the Emergency Roaming Area so that all signatories thereto will be able to understand the Triggering Event's scope and boundaries using universal standard(s) of geography scope recognition (e.g., exchange GIS layers for CENSUS divisions);
b. a description of any potential impacts which the provision of Emergency Roaming may have upon existing commercial wholesale roaming services between the Responding Party and the Receiving Party;
c. reasonable provisions to ensure the Responding Party's networks are not or will not be materially adversely affected by the provision of

Emergency Roaming;

d. clear network management rights and procedures in order to ensure the orderly access and egress of roaming traffic on the Responding Party's network as well as the overall integrity and resiliency of Networks;
e. provisions for:
    i. the Parties to complete any preparations (e.g., establishing or modifying Network interfaces) necessary to enable the efficient provision of Emergency Roaming;
    ii. frequent communication in order to provide situational awareness during a Triggering Event;
    iii. relevant network data exchange as soon as practicable following a Triggering Event;
    iv. coordination of the cessation of Emergency Roaming in order to provide an uninterrupted transition (to the extent possible) back to the Receiving Party's Network for impacted subscribers; and
    v. emergency roaming to be provided to the Receiving Party's wholesale customers if applicable;
f. commercially negotiated fees and payment obligations;
g. as long as the following does not jeopardize a Party's Network, a robust testing regime consisting of (i) technical testing of capabilities, (ii) stress testing, and (iii) introduction of learnings from testing into the development phase of the Emergency Roaming; and
h. Applicable Joint Operating Procedures ("**JOPs**"), if any, developed pursuant to a Bilateral Emergency Roaming Agreement shall be reviewed on a yearly basis and updated as necessary. All Parties shall ensure that applicable JOPs are shared and understood amongst supporting groups within each Party's organization.

Responding Party Indemnity

22. A Receiving Party shall fully and completely indemnify, defend and save harmless a Responding Party and its Affiliates and their respective directors, officers, employees, agents and representatives (the "**Responding Party Indemnitees**") for any direct losses, costs, claims, suits, damages, and awards of any kind incurred by any Responding Party Indemnitees as a result of any third party claim ("**Claim**") resulting from the Responding Party's provision of Emergency Roaming hereunder, excluding any Claims caused by the gross negligence or wilful misconduct of the Responding Party. The indemnity obligations hereunder are conditional on:

a. Receiving Party being provided with written notice of any such Claim;
b. Receiving Party having the right to control and direct the defence of such Claim;
c. Responding Party cooperation with Receiving Party in such defence, at Receiving Party's expense; and
d. Responding Party having the right to be represented in such defence at its expense with advisory counsel of its choice.

Reporting

23. Within thirty (30) days after each Triggering Event's End Point, each Receiving Party and Responding Party shall file a report (an "**Emergency Roaming Report**") in confidence with ISED the CRTC, and CCCS, serving each Party hereto.

24. An Emergency Roaming Report shall report on the following matters:

a. the scope and extent of the events that culminated in the Triggering Event;
b. the nature of Emergency Roaming sought by the Receiving Party;
c. the nature and extent of the Emergency Roaming provided by the Responding Party;
d. any learnings from the Emergency Roaming event that may be useful or that should or should not be repeated, as the case may be, in future

Triggering Events;

e. any thresholds that may be relevant in helping to define the circumstances giving rise to a future Triggering Event; and

f. any other relevant facts associated with that Triggering Event.

25. Joint Post-Event Reports: A Receiving Party and a Responding Party may file a joint Emergency Roaming Report to the extent they agree as to its contents.

26. A Party filing an Emergency Roaming Report may claim confidentiality over certain of its contents on the basis that the designated information: (i) is a trade secret, (ii) contains financial, commercial, scientific or technical information that is confidential and that is treated consistently in a confidential manner by such Party, or (iii) is information the disclosure of which could reasonably be expected to cause material financial loss or gain to any person, prejudice the competitive position of any person or affect contractual or other negotiations of any person. Information in an Emergency Roaming Report that is designated as confidential may be withheld from any other Party. However, for greater certainty, a Party's confidentiality claim is determinative and there shall be no right to appeal or otherwise challenge a Party's confidentiality claim.

Annual Reviews

27. The Parties shall collectively review the effectiveness of this Emergency Roaming Protocol at least once annually, with a view to amending and improving it based upon learnings from the prior year's Triggering Events and information set out in the prior year's Emergency Roaming Report, if any.

Schedule B

Mutual assistance protocol

Purpose:

a. This Mutual Assistance Protocol applies when one or more Parties provides Mutual Assistance to another Party when the latter Party is experiencing a Triggering Event.

Definitions:

2. Unless specifically defined hereunder, capitalized terms shall have the meanings set out in the body of the MOU or Schedule A or Schedule C, as the case may be. In this Mutual Assistance Protocol, the following terms, in singular or plural form according to the context, are defined as follows:

a. "**9-1-1 Network**" means the 9-1-1 core networks operated by Bell, TELUS and SaskTel that transmit 9-1-1 telecommunications to public safety answering points in their respective incumbent local exchange carrier regions.
b. "**Mutual Assistance**" means as stated in Section 3 of this Mutual Assistance Protocol.
c. "**Mutual Assistance Protocol**" means this Schedule B – Mutual Assistance Protocol to the MOU, as it may be amended over time.
d. **"Network"** means a Party's wireline or wireless telecommunications network including, as the case may be, the access network, network core, backhaul, transport connectivity and the infrastructure, in whole or in part.
e. "**Receiving Party**" means a Party that receives Mutual Assistance under this Mutual Assistance Protocol.
f. "**Responding Party**" means a Party that responds to a request for Mutual Assistance under this Mutual Assistance Protocol.

Forms of Mutual Assistance

3. Mutual Assistance may consist of one or more of the following types of temporary assistance, in whole or in part, provided by a Responding Party to a Receiving Party during the entirety, or part of, a Triggering Event, subject to technical feasibility and such reasonable safeguards or terms of use as the Responding Party considers necessary in the circumstances:

a. The sharing of physical assets, such as buildings, and vehicles;
b. The sharing of equipment or logistical support, subject to applicable licensing terms;
c. The sharing of staff or human resources;
d. The provision of one or more services as requested and agreed by both Parties;
e. Access to its 9-1-1 Networks, if applicable;
f. The sharing of licensed spectrum, subject to any necessary authorizations granted by the Minister of Innovation, Science and Industry as may be required by law; and
g. Such other sharing as may be agreed to under the Mutual Assistance Protocol;

For clarity, Mutual Assistance excludes the provision of Emergency Roaming Services (as described in Schedule A to this MOU), Emergency Network Outage Communications Protocol (as described in Schedule C to this MOU) and other forms of assistance not expressly provided for under this Mutual Assistance Protocol.

Principles

4. This Mutual Assistance Protocol shall be invoked by a Party only in case of a Triggering Event and only after having tried, on best efforts basis, to take all possible steps to restore services on its own Network(s). For greater

certainty, a Party shall be prohibited from instigating a Triggering Event as part of that Party's response to operational outages that do not rise to the level of a Critical Network Failure.

5. The provision of Mutual Assistance by a Responding Party is conditional on the Receiving Party taking all possible steps, throughout the Triggering Event Duration, to restore services on its own Network(s) on a best efforts basis.

6. The conduct of a Receiving Party and any Responding Party pursuant to this Mutual Assistance Protocol shall at all times be governed by the duty of good faith.

7. A Responding Party shall attempt to provide Mutual Assistance to the Receiving Party in a Triggering Event for the Triggering Event Duration. However, nothing in this Mutual Assistance Protocol prevents a Party from assisting another Party outside the scope of this Mutual Assistance Protocol.

8. Where a Triggering Event is initiated by a Receiving Party, coincident with the Triggering Event Start Point, or as soon thereafter as reasonably practicable, the Responding Party may request and the Receiving Party shall use reasonable efforts to provide information about the Triggering Event, including: a description of the Critical Network Failure, location(s), estimated duration, identification of any other Parties providing Mutual Assistance and an estimate of the type and quantity of Mutual Assistance required.

9. The Receiving Party and Responding Party shall engage in frequent communication in order to provide situational awareness during a Triggering Event.

10. A Receiving Party shall be required to receive the scope, extent and quality of Mutual Assistance provided by a Responding Party, including the latter's physical assets, staff and services, on an "as is and where is" basis.

For greater certainty there is no duty hereunder upon a Responding Party to augment or supplement the nature and/or quality of its operations and existing Network capabilities to provide Mutual Assistance.

11. A Responding Party is required to provide only such reasonable scope and extent of Mutual Assistance, and only to a level that can be accommodated within its existing capabilities and that will not, in the sole opinion of that Responding Party, materially adversely impact the services it ordinarily provides to its own end-user customers, and to do so where feasible, provided that the Responding Party has reasonably first managed its own Network needs. Without limiting the generality of the foregoing, a Responding Party may, in its sole discretion, decline to provide Mutual Assistance, or withdraw some or all of the Mutual Assistance it had been providing, to the extent the Responding Party is (a) unable to provide, or continue providing, such Mutual Assistance, (b) experiencing a Triggering Event itself, or (c) experiencing or reasonably anticipates experiencing material service degradation due to traffic volumes, network capacity considerations, security events or other factors.

12. In the case where a Triggering Event is followed by one or more Triggering Events, the Parties agree and acknowledge that each Responding Party, as the case may be, shall be required to triage and prioritize the scope and extent of their Mutual Assistance and may reasonably redeploy resources in accordance with the scope and severity of the various Triggering Events.

13. Mutual Assistance shall be wound down and terminated as soon as possible based upon the best efforts of the affected Parties to restore service(s) to their end-user customers and upon the restoration of such services.

14. Where a Responding Party declines to provide, or withdraws, Mutual Assistance, in whole or in part, to a Receiving Party, the Receiving Party shall be entitled to request the reason(s) therefore, and the Responding Party shall provide such reasons in writing.

15. The Parties acknowledge that the provision of Mutual Assistance constitutes the provision of a service to the Receiving Party and the Responding Party is entitled to be compensated by the Receiving Party for its documented reasonable costs and expenses incurred, including at any applicable CRTC tariff rates for the services provided.

Payment

16. The Responding Party may invoice the Receiving Party for its documented reasonable costs and expenses incurred in providing Mutual Assistance under this Mutual Assistance Protocol by way of a standard invoice.

17. Payment from the Receiving Party shall be due in full within 90 days of receipt of the Responding Party's invoice.

18. Billing disputes over any payments hereunder shall be resolved pursuant to Section 20 of the MOU.

Responding Party Indemnity

19. A Receiving Party shall fully and completely indemnify, defend and save harmless a Responding Party and its Affiliates and their respective directors, officers, employees, agents and representatives (the "**Responding Party Indemnitees**") for any direct losses, costs, claims, suits, damages, and awards of any kind incurred by any Responding Party Indemnitees as a result of any third party claim ("Claim") resulting from the Responding Party's

provision of Mutual Assistance hereunder, excluding any Claims caused by the gross negligence or wilful misconduct of the Responding Party. The indemnity obligations hereunder are conditional on:

a. Receiving Party being provided with written notice of any such Claim;
b. Receiving Party having the right to control and direct the defence of such Claim;
c. Responding Party cooperation with Receiving Party in such defence, at Receiving Party's expense; and
d. Responding Party having the right to be represented in such defence at its expense with advisory counsel of its choice.

Reporting

20. Within thirty (30) days after each Triggering Event's End Point, each Receiving Party and Responding Party shall file a report (a "**Mutual Assistance Report**") in confidence with ISED the CRTC, and CCCS, serving each Party hereto.

21. A Mutual Assistance Report shall report on the following matters:

a. the scope and extent of the events that culminated in the Triggering Event;
b. the nature and extent of the Mutual Assistance provided by the Responding Party and received by the Receiving Party;
c. any learnings from the Mutual Assistance event that may be useful or that should or should not be repeated, as the case may be, in future Triggering events;
d. any thresholds that may be relevant in helping to define the circumstances giving rise to a future Triggering Event; and
e. any other relevant facts associated with that Triggering Event.

22. Joint Post-Event Reports: A Receiving Party and a Responding Party may file a joint Mutual Assistance Report to the extent they agree as to its contents.

23. A Party filing a Mutual Assistance Report may claim confidentiality over certain of its contents on the basis that the designated information: (i) is a trade secret, (ii) contains financial, commercial, scientific or technical information that is confidential and that is treated consistently in a confidential manner by such Party, or (iii) is information the disclosure of which could reasonably be expected to cause material financial loss or gain to any person, prejudice the competitive position of any person or affect contractual or other negotiations of any person. Information in a Mutual Assistance Report that is designated as confidential may be withheld from any other Party. However, for greater certainty, a Party's confidentiality claim is determinative and there shall be no right to appeal or otherwise challenge a Party's confidentiality claim.

Annual Reviews

24. The Parties shall collectively review the effectiveness of this Mutual Assistance Protocol at least once annually, with a view to amending and improving it based upon learnings from the prior year's Triggering Events and information set out in the prior year's Mutual Assistance Report.

Schedule C

Emergency Network Outage Communications Protocol

Purpose

1. This Emergency Network Outage Communications Protocol applies during a Triggering Event to ensure that a Party provides the public and Governmental Authorities with the Key Network Outage Information.

Communications under this Emergency Network Outage Communications Protocol are based on the principles of providing timely, relevant and understandable information in a clear and accessible manner.

2. This Emergency Network Outage Communications Protocol applies only in the case of a Triggering Event. For greater certainty, if a Party experiences a Network outage that is not a Triggering Event, then its communications to the public and to Governmental Authorities about such outage is at its sole discretion and not subject to this Emergency Network Outage Communications Protocol.

Definitions

3. Unless specifically defined hereunder, capitalized terms shall have the meanings set out in the MOU or Schedule A or Schedule B, as the case may be. In this Emergency Network Outage Communications Protocol, the following terms, in singular or plural form according to the context, are defined as follows:

a. "**9-1-1 Services**" means voice 9-1-1 services accessed from a wireless or wireline device, where feasible;
b. **"Action Plan"** means a Party's internally approved plans and protocols applicable in the case of a Triggering Event, specifying its communications of Key Network Outage Information to the public and to Governmental Authorities, in accordance with this Emergency Network Outage Communications Protocol;
c. "**Emergency Network Outage Communications Protocol**" means this Schedule C – Emergency Network Outage Communications Protocol to the MOU, as it may be amended over time;
d. "**Key Network Outage Information**" means key available information about the services affected by the Critical Network Failure (other than highly sensitive information that could compromise network security),

the approximate geographic location of the Network outage and the estimated time until Network restoration, as such information may change and become known over the course of the Critical Network Failure;

e. "**Network**" means a Party's wireline or wireless telecommunications network including, as the case may be, the access network, network core, backhaul, transport connectivity and the infrastructure, in whole or in part;

Principles

4. Parties agree to inform the public and Governmental Authorities about the Key Network Outage Information in accordance with their respective Action Plans.

5. Parties should ensure that they have sufficient back-up systems and processes in place to enable their communications to the public and to Governmental Authorities in the event of a Triggering Event.

6. The conduct of each Party pursuant to this Emergency Network Outage Communications Protocol shall at all times be governed by the duty of good faith.

Protocols

7. **Preparation for a Triggering Event**: In preparation for a Triggering Event, each Party agrees to do the following:

a. prepare an Action Plan that sets out its communications policies and procedures applicable during a Critical Network Failure, which Action Plan must have the Party's leadership approval within 90 days of the Effective Date;
b. set out tailored policies and procedures that the Party will follow during a Critical Network Failure;

c. ensure access is available by a Party's representatives responsible for communications under this Emergency Network Outage Communications Protocol to telecommunications via alternative networks to ensure that they can conduct two-way communications and access electronic communications in the event of a Critical Network Failure that prevents that Party from connecting to its own Networks or from authenticating its identification via its own Networks; and
d. review its Action Plan on at least an annual basis, to ensure it remains effective and consistent with this Emergency Network Outage Communications Protocol.

Communication of a Critical Network Failure to the Public: Throughout the Triggering Event Duration a Party will use commercially reasonable efforts to:

a. inform the public of the Key Network Outage Information, and any such communications must include information about whether access to 9-1-1 Services is affected;
b. provide information to the public about the Key Network Outage Information within two (2) hours of the Party issuing a Triggering Event Declaration or as expeditiously as possible;
c. make the Key Network Outage Information available electronically via its website and other electronic means, if available, in accordance with its Action Plan and applicable accessibility laws;
d. endeavor to provide updates using the tools identified in 8(c) about the outage as the status of any information about the Key Network Outage Information changes;
e. upon the Triggering Event End Point, notify the public electronically using the tools identified in 8(c) that the Triggering Event has concluded.

Communications to Governmental Authorities During a Network Outage: Throughout the Triggering Event Duration, a Party will use commercially reasonable efforts to:

a. inform Governmental Authorities of the Key Network Outage Information, and any such communications must include information about whether access to 9-1-1 Services is affected;
b. provide information to the Governmental Authorities about the Key Network Outage Information within two (2) hours of the Party becoming aware of the Triggering Event or as expeditiously as possible;
c. provide communications to the Governmental Authorities in such manner that the Party determines to be the most reasonable and effective means for each of the Governmental Authorities;
d. endeavor to provide timely updates about the outage as the status of any of the Key Network Outage Information changes;
e. upon the Triggering Event End Point, notify the Governmental Authorities of this information in such manner that it determines to be the most reasonable and effective means, as soon as reasonably possible.

Schedule D

Parties to the MOU

a. **BELL CANADA** ("**Bell**"), a corporation organized under the laws of Canada and having its principal place of business at 1 Carrefour Alexander-Graham-Bell, Building A-7, Verdun, Quebec, H3E 3B3;
    - Signed: September 6, 2022
    - Signatory: Mirko Bibic, President and Chief Executive Officer
b. **BRAGG COMMUNICATIONS INC.** ("**Eastlink**"), a corporation organized under the laws of the Province of Nova Scotia and having its principal

place of business at 6080 Young Street, 8th Floor, Halifax, Nova Scotia, B3K 5L2;

- Signed: September 1, 2022
- Signatory: Lee Brag, Executive Vice Chair

c. **COGECO COMMUNICATIONS INC.** ("**Cogeco**"), a corporation organized under the laws of Canada and having its principal place of business at 1, Place Ville-Marie, bureau 3301, Montréal, Québec H3B 3N2;

- Signed: September 6, 2022
- Signatory: Philippe Jetté, President and Chief Executive Officer

d. **ROGERS COMMUNICATIONS CANADA INC.** ("**Rogers**"), a corporation organized under the laws of Canada and having its principal place of business at 333 Bloor Street East, Toronto, Ontario M4W 1G9;

- Signed: September 1, 2022
- Signatory: Anthony Staffieri, President and Chief Executive Officer

e. **SASKATCHEWAN TELECOMMUNICATIONS** ("**SaskTel**"), a corporation existing pursuant to its own statute and having its principal place of business at 2121 Saskatchewan Drive, Regina, Saskatchewan;

- Signed: September 2, 2022
- Signatory: Doug Burnett, President and Chief Executive Officer

f. **SHAW COMMUNICATIONS INC.**, a corporation existing under the laws of the Province of Alberta and having its principal place of business at 900, 630 – 3rd Avenue S.W., Calgary, Alberta, T2P 4L4, and its Affiliate **FREEDOM MOBILE INC.**, a corporation existing under the laws of the Province of Alberta and having its principal place of business at 16 York Street, Toronto, Ontario, M5J 0E6 (together, "**Shaw**");

- Signed: September 6, 2022
- Signatory: Brad Shaw, Executive Chair and Chief Executive Officer

g. **TBAYTEL** ("**Tbaytel**"), a company organized under the laws of Canada and having its principal place of business at 1046 Lithium Drive, Thunder Bay, Ontario, P7B 6G3;

- Signed: September 6, 2022
- Signatory: Daniel Topatigh, President and Chief Executive Officer

h. **TELESAT CANADA** ("**Telesat**"), a corporation organized under the laws of Canada and having its principal place of business at 160 Elgin Street, Suite 2100, Ottawa, Ontario, H2K 4P7;

- Signed: September 1, 2022
- Signatory: Christopher DiFrancesco, VP, General Counsel & Secretary

i. **TELUS COMMUNICATIONS INC.** ("**TELUS**"), a corporation organized under the laws of the Province of British Columbia and having its principal place of business at 7th Floor, 510 West Georgia Street, Vancouver, British Columbia, V6B 0M3;

1. Signed: September 2, 2022
2. Signatory: Darren Entwistle, President and Chief Executive Officer

j. **VIDEOTRON LTD.** ("**Videotron**"), a corporation organized under the laws of the Province of Quebec and having its principal place of business at 612, St-Jacques Street, Montreal, Quebec, H3C 4M8;

- Signed: September 6, 2022
- Signatories: Pierre Karl Péladeau, President

k. **XPLORNET COMMUNICATIONS INC.** ("**Xplornet**"), a corporation organized under the laws of the Province of New Brunswick and having its principal place of business at 300 Lockhart Mill Road, Woodstock, New Brunswick, E7M 6B5; and

- Signed: September 2, 2022
- Signatory: Allison Lenehan, President and Chief Executive Officer

l. **ZAYO CANADA INC.** ("**Zayo**"), a corporation organized under the laws of Ontario and having its principal place of business at 5160 Orbitor Dr, Mississauga, Ontario L4W 5H2.

- Signed: September 6, 2022
- Signatory: Michael Strople, Managing Director Zayo Canada

PUBLIC

Schedule E

Notice addresses

Party:	Notice address:
Bell	Bell Canada Corporate Secretary 1 Carrefour Alexander-Graham-Bell, Building A-7 Verdun, Quebec, H3E 3B3 Attention: Corporate Secretary Email: corporate.secretariat@bell.ca Email: bell.regulatory@bell.ca
Eastlink	Bragg Communications Inc. Legal Department 6080 Young Street, 9th Floor Halifax, Nova Scotia, B3K 5L2 Email: Legal.Matters@corp.eastlink.ca Email: Regulatory.Matters@corp.eastlink.ca
Cogeco	Cogeco Communications Inc. Legal Department 1, Place Ville-Marie, bureau 3301 Montréal, Québec H3B 3N2

PUBLIC

Rogers	Rogers Communications Canada Inc. Regulatory Department 333 Bloor Street East Toronto, Ontario M4W 1G9 Attention: VP, Regulatory Email: Regulatory@rci.rogers.com With a copy to: Rogers Communications Canada Inc. Legal Department 333 Bloor Street East Toronto, Ontario M4W 1G9 Attention: VP, Legal Email: legal.contracts@rci.rogers.com
SaskTel	Saskatchewan Telecommunications 13th Floor, 2121 Saskatchewan Drive Regina, SK SP3Y2 Attention: Chief Technology Officer With a copy to: Saskatchewan Telecommunications 13th Floor, 2121 Saskatchewan Drive Regina, SK SP3Y2 Attention: VP – Legal and Regulatory Affairs
Shaw	Shaw Communications Inc. Legal Department 900, 630 3rd Avenue SW Calgary, Alberta T2P 4L4 Attention: Chief Legal Officer Email: sclegal@sjrb.ca

PUBLIC

Tbaytel	Tbaytel Regulatory Department 1046 Lithium Drive Thunder Bay, Ontario, P7B 6G3 Email: TBTRegulatory@tbaytel.com
Télésat	Telesat Canada c/o: Corporate Secretary 160 Elgin Street, Suite 2100 Ottawa, ON, H2K 4P7 Email: contract-notice@telesat.com
TELUS	TELUS Communications Inc. 29th Floor, 25 York Street Toronto, Ontario, M5J 2V5 Attention: Contracts Department Email: gt&ps.contracts@telus.com With a copy to: TELUS Communications Inc. 29th Floor, 25 York Street Toronto, Ontario M5J 2V5 Attention: Director – Products & Services Email: david.morrow@telus.com

Vidéotron	Videotron Ltd. 612 St-Jacques Montreal, Québec H3C 4M8 Attention: VP, Legal Affairs Email: legalnotice@quebecor.com With a copy to: Videotron Ltd. Roaming Department 612 St-Jacques Montréal, Québec H3C 4M8 Attention: Senior Director Email: roaming.coordinator@videotron.com
Xplornet	Xplornet Communications Inc. 625 Cochrane Drive, Suite 1000 Markham, Ontario L3R 9R9 Attention: Chief Legal and Regulatory Officer Email: Xplornet.Legal@corp.xplornet.com
Zayo	Zayo Group Attn: Underlying Rights/Legal 1401 Wynkoop Street, Suite 500 Denver, CO 80202 legal@zayo.com

Date modified:
2022-09-07