Ted Woodhead

Rogers Communications Inc.
360 Albert Street, Suite 830
Ottawa, Ontario K1R 7X7
ted.woodhead@rci.rogers.com
m 613.220.7575

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:

#

#

#

#

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

#

#

#

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:

#

#

(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:

#

Filed in Confidence with the Commission

#

(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 #
#

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 #

#

- 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. #
  .
- 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. #
  #
- 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. #
  #
- 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 # # 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. #
  #
- 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. #
  #

(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: #
#

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

#), 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 #

#

(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:

#

#

#

(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:

#

#

#

#

Filed in Confidence with the Commission

#

#

#

#

#

#

(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;

Filed in Confidence with the Commission

#

#

#

#

#

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 # # 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):

#

#

#

#

#

#

#

#

#

#

#

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

Rogers' priority sequence for service restoral was as follows:

#

#

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. #

#

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

#

Filed in Confidence with the Commission

#

#

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:

#

#

#

#

#

#

#

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:

#

#

#

#

(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, # # 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.

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

Filed in Confidence with the Commission

#

#

#

#

#

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 (# #). 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 # #. 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.

#.

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:

#

#

#

#

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,

#
#

(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.

#
#.

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 # # 9-1-1 calls placed successfully across Rogers' network on July 8th. The typical daily average of total wireline 9-1-1 calls is # # per day. Data is unavailable for unsuccessful wireline 9-1-1 calls. On July 9th, there were approximately # # 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 # # the average daily amount of about # # 9-1-1 calls made from Rogers wireless devices.
#

#	#	#	#
#	#	#	#
#	#	#	#
#	#[1]	#	#[2]
#	#	#	#

*** 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. # # 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. # #. 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 # #.

(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 # #. However, as discussed in Rogers(CRTC)11July2022-2.i above, some # # calls were completed on Rogers' wireless network, # # an average day's number of calls.

On an average day, Rogers wireless customers place # # 9-1-1 calls, of which # # are successful and # # 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.

#

#[3]	

[3] A 30-second call duration was selected to identify successfully completed calls to a PSAP during the outage (i.e. # # 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;

Filed in Confidence with the Commission

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 # # 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 # # completed 9-1-1 calls and TELUS # #. As such, Rogers believes that approximately # # 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 # #. 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 (# #). 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 # #. In term of specific measures and safeguards, we assessed and addressed the following items:
#

#

#

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 # #. 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 # #). Lastly, since # #, 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 # #.

Finally, # #.

Filed in Confidence with the Commission

*** End of Document ***

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 ***