



28 July 2026

Marc Morin
Secretary General
CRTC
Ottawa, ON K1A 0N2

Filed online

Dear Secretary General,

Re: TELUS Communications Inc., *Part 1 Application Seeking Interim Relief and Commission Review of the Wireless Device Unlocking Requirements under the Wireless Code*, [Part 1 Application 8665-T66-202603464](#) (Gatineau, 11 June 2026)

The Forum for Research and Policy in Communications (FRPC) is a non-profit and non-partisan organization established in 2013 to undertake research and policy analysis about communications, including broadcasting and telecommunications.

FRPC's intervention in this proceeding are attached. We look forward to the opportunity to review the company's reply, and to its submissions regarding the permanent relief this application seeks in the CRTC's 2026-134 proceeding by amending the *Wireless Code* (pursuant to the [CRTC staff's letter of 8 July 2026](#)).

Sincerely yours,

Monica Auer, M.A., LL.M.
Executive Director
Ottawa, Ontario

execdir@frpc.net



Nine years after the CRTC prohibited device-locking, TELUS asks for a re-do: without relevant evidence, proportionality or efficiency

TELUS Communications Inc., *Part 1 Application Seeking Interim Relief and Commission Review of the Wireless Device Unlocking Requirements under the Wireless Code*, [Part 1 Application 8665-T66-202603464](#) (Gatineau, 11 June 2026)

Intervention
by the
Forum for Research and Policy in Communications (FRPC)

28 July 2026



Contents

Executive Summary	1
I. Introduction	1
A. From wireless to wireless	1
B. Surge in wireless complaints lead to 2013 <i>Wireless Code</i> and 90-day device locks	2
C. Telcos, not miscreants, killed the goose in 2017	4
II. TELUS' 2026 application	6
A. Stale evidence	6
B. Excessive redaction	6
C. Proposal's inefficiency highlighted by TELUS' SIM swap issue	7
III. Six reasons to deny TELUS' device-locking proposals	8
A. The CRTC rejected Bell's device-locking proposal eight months ago	8
B. Device-locking nullifies the 15-day trial period	9
C. Device-locking unlikely to reduce or prevent theft	10
D. Device-locking converts owned devices into rentals	12
E. Device-locking puts Canadians at risk	13
1. A Locked Phone Undermines the "9-1-1 Safety Net"	13
2. Locked devices block non-9-1-1 calls for help	13
F. Device-locking introduces biometric identity authentication	14
1. A new barrier	15
2. A significant invasion of privacy	15
IV. Concerns about the impact of granting TELUS' interim-relief application ...	16
A. Relying on existing procedural rights may trigger device-locking	16
B. Device-locking as boundary testing	17
C. Interim steps may lead to permanent changes	18
V. Conclusions and recommendations	18
A. Effective and less restrictive alternatives exist, including Rogers' "smart safe"	19
B. Recommendations	19
Figures	
Figure 1 Wireline and wireless penetration rates, 1947-2015	2
Figure 2 Rogers' retail outlet in Ottawa (July 2026)	10
Appendices	
Appendix 1 CRTC's 8 July 2026 Staff Letter to TELUS	1
Appendix 2 Theft of cellphone devices: pickpocketing	3



Executive Summary

- ES 1** This intervention strongly opposes the Part 1 application by TELUS Communications Inc. (TELUS) for the CRTC to reinstate the device-locking practice the CRTC prohibited in 2017 so as to
- reduce market confusion and bill shock,
 - simplify the CCTS' administration of the Wireless Code,
 - improve device portability and reduce barriers to switching WSPs,
 - offer consumers more choice, more convenience and more dynamism in the market, and to give all consumers fair, consumer-friendly treatment.
- ES 2** FRPC supports – indeed, who would oppose? - legitimate measures to protect the safety of retail staff and stores and to mitigate fraud. Yet the evidence TELUS provides to support its claims of rampant, violent theft in its stores is seven years old and refuted by the company itself: TELUS says that in today's world, theft is taking place in the wireless-device supply chain while SIM swap fraud is occurring due to weaknesses in its customer-verification systems.
- ES 3** Re-introducing all the harms that the CRTC blocked in 2017 by disallowing device-locking will not benefit consumers, contravenes Parliament's telecommunications policy and Cabinet's 2023 *Direction*. FRPC notes that TELUS application – which would apply on an interim basis to all WSPs – either redacts relevant evidence, limiting both verification and challenge or fails to provide it, is wildly disproportionate as a means of limiting street-level theft and is an entirely inefficient way to reduce SIM swap fraud, given that device-locking has nothing to do with fraudsters' deception of WSPs.
- ES 4** Worse, granting TELUS' proposal would violate the *Wireless Code's* consumer-protection mandate while actively placing the public safety of Canadians and First Nations peoples living in rural areas full-time or seasonally at risk (since they will be unable to determine objectively whether the devices they have just obtained through TELUS actually work for them and serve their needs – including the ability to receive emergency alerts at all times. Rather than safeguarding the public and serving the public interest, granting TELUS proposal would place Canadians at risk, a clear disservice to the public interest.
- ES 5** Even worse, allowing WSPs to harvest new subscribers' biometric data – ostensibly to more easily detect fraud – not only ignores Canadians' *Charter*-protected privacy rights and Canadian privacy law, but could enable the creation of a new 'normal' through a small incremental step in harvesting the biometric information of millions of wireless subscribers through the innocuous device of a part 1 telecommunications application

ostensibly seeking to reduce violent crime for which no current, Canadian evidence is provided.

ES 6 Moreover,

- a. TELUS has not explained why the CRTC, having [decided on 28 November 2025](#) that a 60-day lock is “not in the best interest of consumers” and is not a demonstrably “necessary and proportionate response” should now grant TELUS interim application to the benefit of all WSPs, despite the absence of either new facts or compelling need;
- b. TELUS has not demonstrated that retailers’ current physical security measures such as time-activated smart safes are ineffective in mitigating retail theft;
- c. TELUS has not explained why it is proposing to implement biometric-identification requirements for subscribers seeking early device unblocking, how such requirements will be met (samples of tissue, blood or hair, for example, or ‘merely’ fingerprints?), why such requirements do not breach Canadians’ *Charter*-based right to privacy or why a Part 1 application for interim relief is an appropriate mechanism for the CRTC to approve a breach of Parliament’s objective that Canadian telecommunications should “contribute to” not reduce “the protection of the privacy of persons”;
- d. TELUS has not explained why consumers’ interest in verifying network coverage where they require it using the only empirical tool they have – swapping in a competitor’s SIM chip within the legally mandated 15-day return window – should be overborne by unproven claims. Nor has TELUS explained why any advantage it gains exceeds the clear public-safety disadvantages when locked devices prevent users in locations with volatile or inaccurate coverage maps from ensuring that they can receive NPAS alerts, localized disaster warnings and calls to check wellbeing. These disadvantages are particularly acute for First Nations communities that lack 9-1-1 service altogether and for low-income or elderly people;
- e. TELUS has not explained how device-locking will affect users’ access to emergency services (separate from 9-1-1), telephone welfare checks and localized disaster warnings, nor has it explained the impact of its proposal on First Nations communities that may in some cases lack 9-1-1 service altogether;
- f. TELUS has not explained how device-locking will reduce or prevent street-level crimes such as pickpocketing and distraction theft in which stolen devices are not sold for use but are disassembled for the income generated by selling the parts;
- g. TELUS’ proposal effectively converts a purchased device into a rental, the unacceptable state of affairs that the CRTC corrected when it amended the *Wireless Code* in 2013. While shifting all financial risk to the consumer through the transfer of title to the device, companies’ device-locking enables them to control consumers’ use of and rights to the device they ‘own’.



- ES 7** The CRTC should deny TELUS interim application for the reasons stated above.
- ES 8** If the CRTC decides to grant any form of TELUS' proposal for device locking, it should in the alternative
- a.** mandate that any anti-theft locking mechanism be automatically and instantly deactivated via Point-of-Sale Whitelisting as soon as a consumer transaction is completed;
 - b.** Extend the current 15-day trial period to at least 75 days to account for the 60-day lock and to provide consumers with a meaningful opportunity to test network service that is not always available as hoped;
 - c.** require carriers to offer a clear, enforceable and enforced "Anti-Theft Guarantee" through which the carrier assumes liability for fraud or theft during the lock period, shifting the risk to the company from consumers whose devices are locked; and
 - d.** require carriers to guarantee seamless access to all emergency and non-emergency communication channels—including 10-digit emergency numbers, the Alert Ready system, and incoming voice communications—during the device-locking period and while services may be down for that particular provider.
- ES 9** The CRTC should also
- a.** clarify the scope of this proceeding to expressly include consideration of whether TELUS's proposed use of biometric identity authentication (is a "necessary and proportionate" measure, or in the alternative, state that no reliance will be placed on paragraph 124(c) in determining whether the interim relief should be granted,
 - b.** issue a public warning consistent with the Commission's [28 November 2025](#) warning to Bell that any carrier implementing a device lock without the CRTC's express authorization will be subject to enforcement action, including Administrative Monetary Penalties (AMPs), and
 - c.** order carriers to utilize less restrictive means, such as the National IMEI Blacklist and physical retail security infrastructure (e.g., time-activated smart safes), to resolve corporate shrinkage issues without penalizing consumer property rights.
- ES 10** To ensure that all Canadians have a reasonable opportunity to comment on this issue, the CRTC should also amend Notice of Consultation 2026-134 to state clearly that TELUS is asking to remove the device-locking prohibition from the *Wireless Code*, that interested parties may comment on this proposal and that parties may also propose changes to any or of the *Codes* addressed by 2026-134.

I. Introduction

1. The Forum for Research and Policy in Communications (FRPC) is a non-profit and non-partisan organization established in 2013 to undertake research and policy analysis about communications, including broadcasting and telecommunications.
2. On 22 May 2026 TELUS Communications Inc. (TELUS) asked the CRTC to give “temporary and permanent authorization” to all wireless service providers in Canada to impose 60-day locks on devices purchased by their customers
3. FRPC opposes approval of TELUS’ application.
4. The Forum outlines the context of device-locking in the remainder of this Part. Part II sets out eight reasons for denying TELUS’ application. In Part III FRPC points out two negative consequences for consumers that, while hypothetical, are based in past behaviour. Part IV sets out FRPC’s conclusions and recommendations.

A. From wireless to wireless

5. Wireless telephone services have operated for close to a century.¹ Following on the heels of Mexico, Saudi Arabia, Sweden, Norway, Denmark and Sweden,² Canada’s Department of Communications called for cellular mobile applications in mid-October 1982.³

[Remainder of page left intentionally blank]

¹ In 1946 AT&T launched a commercial mobile radio-telephone service in Missouri, in which a “centrally located antenna transmitted to mobiles [mobile telephone sets], all of them car based radio-telephones Waiting lists developed immediately in every one of the twenty five cities MTS [mobile telephone service] was introduced.” Tom Farley, “Mobile Telephone History” in “Future Mobile Phones”, *Teletronikk* Vol.101 (3/4), 2005, http://www.telenor.com/wp-content/uploads/2012/05/T05_3-4.pdf#page=24, 22-34 at 23-24.

In 1953 a published journal article addressed the principles underlying cellular radio. (*Ibid.*).

By “1964 the Bell System introduced Improved Mobile Telephone Service or IMTS, a replacement to their badly aging Mobile Telephone System.7) With IMTS people didn’t have to press a button to talk. Conversations went back and forth just like a regular telephone” (*Ibid.*, at 24), and in 1973 the first public cellphone call took place: CBC news, “5 major moments in cellphone history: Motorola engineer Martin Cooper made first public cellphone call on April 3, 1973”, (3 April 2013) <http://www.cbc.ca/news/technology/5-major-moments-in-cellphone-history-1.1407352>: “Cooper made the call on a New York City street in front of reporters from a device weighing about 1½ kilograms. Motorola spent almost \$1 million producing the phone, Cooper later told the BBC. Cost of the phone for a consumer — when it became available 10 years later — would have been equal to almost \$9,970 in today’s currency.”

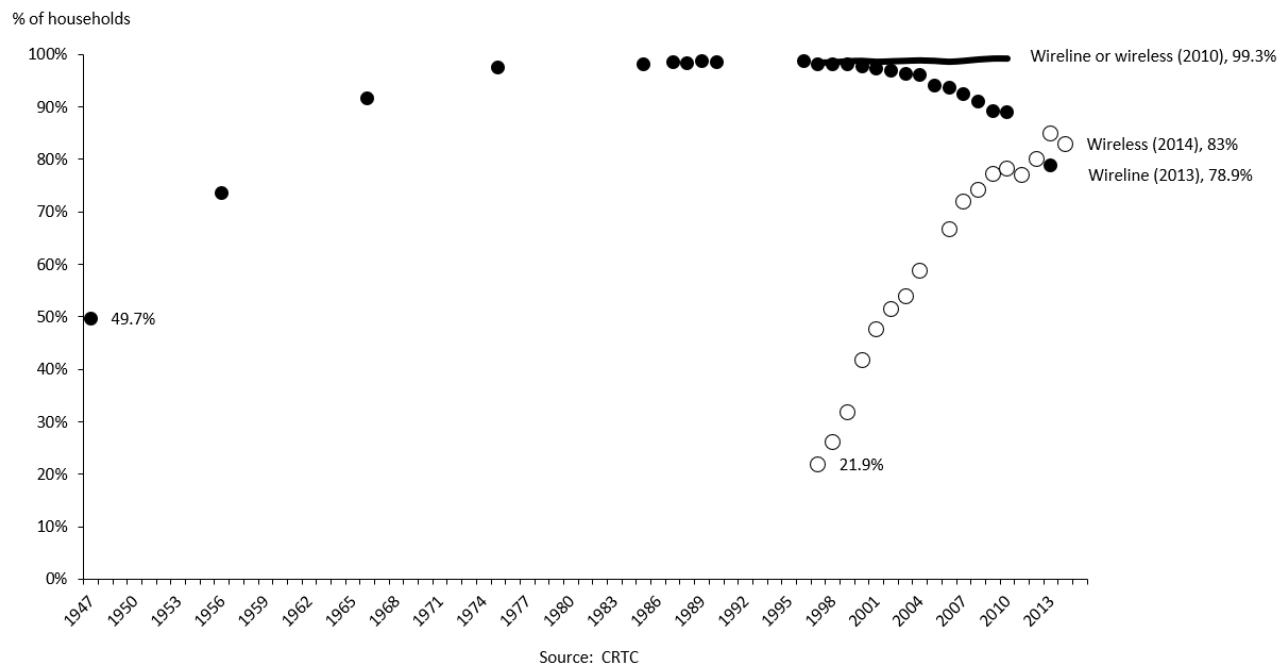
² *Supra* note 1, Tom Farley at 24.

³ Spectrum Management and Telecommunications Policy, Industry Canada, ISED, *A Brief History of Cellular and PCS Licensing*, October 2004, at 1.

6. It's fair to say that Canadians relished the chance to stay in touch with family, friends, colleagues and others without being tied to cords. By the early 2010s the percentage of Canadians who subscribed to mobile wireless exceeded the percentage subscribing to wireline telephone services (84.9% vs 78.9%⁴): Figure 1.⁵

Figure 1 Wireline and wireless penetration rates, 1947-2015

Telephone penetration rates in Canada, 1947-2015



- B. Surge in wireless complaints lead to 2013 *Wireless Code* and 90-day device locks
7. By 2011 complaints about wireless services made up 62% of all complaints received.⁶ A year later the CRTC decided that while conditions in the retail wireless market had not changed enough for it to fully regulate in this sector, it retained the power “to impose any conditions on the offering and provision of any telecommunications service by a

⁴ CRTC, *Communications Monitoring Report (CMR) 2015*, page 1.

⁵ 1947-1990: CRTC, Annual Report, 1990-1991, p. 32 ("Telephone Penetration Rates (percentage)"); 1996: CRTC, Departmental Performance Report 1998, p. 31; 1997=2001: CRTC, Rapport a la gouverneure en conseil, (Nov. 2003), at 11, Table 3.4; 2002-2005: CRTC Telecommunications Monitoring Report (July 2006) at 6, Table 2.3.1; 2005-2006: CRTC Telecommunications Monitoring Report 2007, at 8, Table 2.3.1; 2010-2014: CMR 2015, Figure 5.5.8 (Mobile device penetration).

⁶ CRTC, *Communications Monitoring Report 2012*, page 10; the CCTS received 690 complaints about wireless telecommunications services in 2008 and 4,964 such complaints (619% more) in 2011 (page 13, Table 2.2.5).

Canadian carrier”.⁷ It noted “the significant consumer concerns raised by individuals, consumer groups, and mobile WSPs with respect to the clarity of mobile wireless contracts and launched a proceeding

... to establish a mandatory code to address the clarity and content of mobile wireless service contracts and related issues, to ensure that consumers have the information and protection they need to make informed choices in the competitive market.”⁸

8. PIAC stated that “Consumers should be able to use their devices unlocked from the day that they receive them.”⁹ Consumers Council of Canada supported PIAC’s position, arguing that

159 Unless WSPs present evidence that breach of contract is so widespread and has seriously negative consequences that exceed the normal costs of business that it cannot be addressed through the proper legal routes, the cross-Canada Wireless Code should restrict or eliminate device locking altogether. ...

9. TELUS did not appear at the CRTC’s *Wireless Code* public hearing. Its final written submission confirmed that “consumer wireless devices in Canada are almost universally ordered, manufactured, and sold to consumers locked to the network on which they are initially intended to be used.”¹⁰
10. TELUS then said that it “supports a rule that service providers have to offer device unlocking on reasonable terms for those customers who desire it” – but that “mandating that all devices be sold unlocked or immediately unlockable would have several negative consequences for consumers and service providers alike.”¹¹ Specifically, TELUS said that device-locking “helps ensure” Canadians’ timely and affordable access to “world class handsets”¹² because locking prevents abuse.¹³ It also said that if it were forced to sell unlocked devices, ““scalpers” could buy the devices from us and turn around and sell them at a much higher price (either in Canada or other countries)”.¹⁴

⁷ *Decision on whether the conditions in the mobile wireless market have changed sufficiently to warrant Commission intervention with respect to mobile wireless services*, [Telecom Decision CRTC 2012-556](#) (Ottawa, 11 October 2012), at ¶122.

⁸ *Decision on whether the conditions in the mobile wireless market have changed sufficiently to warrant Commission intervention with respect to mobile wireless services*, [Telecom Decision CRTC 2012-556](#) (Ottawa, 11 October 2012), at ¶127.

⁹ PIAC, *Final Written Comments of PIAC/CAC/COSCO*, (Ottawa, 1 March 2013), Appendix A: Consumer and Public Interest Groups Consensus Positions on the draft Wireless Code, point 7.

¹⁰ TELUS, *FINAL WRITTEN COMMENTS OF TELUS CNS COMPANY*, (Ottawa, 1 March 2013) at ¶122.

¹¹ *Ibid.*, at ¶124.

¹² *Ibid.*

¹³ *Ibid.*, at ¶¶125-126, citing WIND Mobile.

¹⁴ On this point TELUS (¶128) also cited MTS:

11. TELUS later clarified that “[t]he main reason for the 90-day period – as MTS explained – is so we can establish the customer’s good credit history.”¹⁵
12. The CRTC established the *Wireless Code* in 2013 “to empower consumers in their relationships with their wireless and television service providers.”¹⁶ It considered 19 issues concerning the *Code*’s content: locked wireless devices “was one of the most significant sources of consumer frustration with wireless services”.¹⁷
13. The CRTC concluded that device-locking “can be a barrier for customers who want to migrate to a competing WSP or subscribe to services from a foreign WSP while travelling abroad”.
14. But the Commission noted that WSPs had provided evidence that locking may in some circumstances “limit subscription fraud”.¹⁸ It therefore decided to let WSPs lock devices temporarily – but said they should then “make an unlocking service available to customers who have been subscribed to their services for 90 days”, “to mitigate any risks associated with unlocked devices”.¹⁹
15. The CRTC then decided to review the *Wireless Code* in 2016.²⁰

C. Telcos, not miscreants, killed the goose in 2017

16. The public record of the 2016/17 *Wireless Code* review shows that the CRTC heard very clearly from wireless customers. The CRTC’s June 2017 decision noted that

... Individuals and consumer groups generally submitted that unlocking fees were too high or should be prohibited, arguing that WSPs should bear the cost of

We prefer locked for a number of reasons. Principally it helps us manage risk. There’s inventory risk, so, having locked devices while they’re in inventory helps protect the device. It also helps us manage risk during the initial phase because, you know, if you have an unlocked device, potentially you’re more vulnerable to subscription fraud, people coming in, taking essentially a zero dollar device and then never paying a bill and having difficulty, you know, because the device is unlocked from day one or within a very short period of time. So, there’s that issue.

And then, I think generally speaking though that, you know, we feel after 90 days we’ve got a track record, the customer’s paid, you know, at least one bill, probably two bills and if they come in and their account is in good standing, we’re fine to unlock the phone.

¹⁵ TELUS, at ¶129.

¹⁶ CRTC, [Report on Misleading or Aggressive Communications Retail Sales Practices](#), (Ottawa, 2019) ISSN: 978-0-660-29622-7, Cat. No.: BC92-103/2019E-PDF, at 23 of 39.

¹⁷ *Ibid.*, at ¶152.

¹⁸ *Ibid.*, at ¶162.

¹⁹ *Ibid.*, at ¶163.

²⁰ *Review of the Wireless Code*, [Telecom Notice of Consultation CRTC 2016-293](#) (Ottawa, 28 July 2016).

unlocking phones from their networks as a cost of doing business, or they should not lock devices in the first place.

WSPs generally argued that they should be permitted to continue locking devices, and that no conditions should be placed on their ability to levy charges for unlocking ²¹

... Some individuals stated that the locked status of their phone was a disincentive from participating in the second-hand device market or from passing along used phones to family members.²²

...

Freedom Mobile viewed current WSP practices regarding locking to be a major inconvenience and a barrier to switching WSPs for the customer.²³

...

Some individuals expressed frustration that devices they had purchased unlocked from a manufacturer became locked to a WSP's network once a SIM card was inserted.²⁴

...

17. As before in 2013, the CRTC in 2017 found that “the provision of locked devices was one of the most significant sources of consumer frustration with wireless services.”²⁵ It noted that WSPs “verify the identity and credit history of customers through credit checks or by requiring security deposits”,²⁶ that “empirical evidence” supporting a connection between unlocked wireless phones and unpaid bill amounts “was minimal”²⁷ and that WSPs can use the international mobile equipment identity numbers (IMEI numbers) to deter the resale of devices stole from their retail outlets or obtained through fraud.²⁸

18. The Commission decided not to permit device-locking to

- “ensure that customers have the benefit of unlocked devices” going forward (¶306)
- reduce market confusion (¶307)
- simplify the *Wireless Code*'s administration by the CCTS (¶307)

²¹ *Review of the Wireless Code*, Telecom Regulatory Policy CRTC 2017-200 (Ottawa, 15 June 2016), at ¶¶262-263.

²² *Ibid.*, ¶264.

²³ *Ibid.*, ¶266.

²⁴ *Ibid.*, ¶269.

²⁵ *Ibid.*, ¶296.

²⁶ *Ibid.*, ¶301.

²⁷ *Ibid.*

²⁸ *Ibid.*, ¶302.

- improve device portability and therefore barriers to switching WSPs (¶298, ¶300)
- offering consumers more choice and convenience (¶298)
- promote dynamic marketplace development (¶298)
- treat existing customers with locked devices fairly and in a “consumer-friendly” way (¶307)
- reduce the risk of customers’ bill shock while travelling abroad (¶298, ¶299), and
- improve the reliability and effectiveness of “third-party device unlocking” (¶305).

19. In mid-June 2017 Telecom Decision CRTC 2017-200 prohibited device-locking practices effective 1 December 2017.²⁹

II. TELUS’ 2026 application

20. Section 22(2)(e) of the 2010 *Canadian Radio-television and Telecommunications Commission Rules of Practice and Procedure* requires parties to submit relevant facts in support of their arguments. The Commission's November 28, 2025, Bell decision explicitly found that Bell had not demonstrated that a 60-day lock was “necessary and proportionate.” Similarly, TELUS is asking the Commission to grant a significant regulatory change based on claims it is unwilling or unable to substantiate.

A. Stale evidence

21. TELUS argues that device unlocking must be re-introduced because organized and opportunistic criminals find portable unlocked mobile devices to be attractive and “quickly resold” (¶12). It argues that “[s]martphones are extremely valuable right now” (¶12), claims that resellable mobile devices without locking safeguards are “directly compromising the safety of retail employees, small businesses, and the public” (¶12) and says that armed thieves rob stores by filling bags with smartphones (¶13).

22. TELUS supports these three statements using the same news item – from 2019, seven years ago.³⁰

B. Excessive redaction

23. The remainder of TELUS's application appears to rely on redacted data and unsubstantiated claims. The key evidence of its own fraud losses (¶¶ 8, 11(b), 32, 33, 35,

²⁹ *Ibid.*, ¶311.

³⁰ CBC News, “Police charge 22 in rash of cellphone store robberies in Greater Toronto Area” (12 June 2019), online: <https://www.cbc.ca/news/canada/toronto/cellphone-store-robberies-greater-toronto-area-matrix-bandits-toronto-police-hold-up-squad-1.5172465>.

84, 86, 105, 114, 115, 158), the effectiveness of the lock (¶24, Figure 1, Figure 2), and the benefits to consumers (¶84) is almost entirely redacted. .

24. Redactions of this scale make it difficult if not impossible for the public to verify or challenge necessary evidence. Absent public, verifiable evidence, it would be difficult for the CRTC to find that the proposed 60-day device-locking practice is "necessary and proportionate" for TELUS or, indeed, for all WSPs. The application should be denied on this basis alone."

C. Proposal's inefficiency highlighted by TELUS' SIM swap issue

25. FRPC also notes that TELUS's application also appears to acknowledge a severe Sim Swap fraud issue also known as "account takeover fraud" (¶105). TELUS knows that it is losing devices through this fraud vector ("takeover"). SIM swap fraud is an internal security failure that, as TELUS itself explains, "occurs when a fraudster convinces your mobile provider to transfer your mobile phone number to a new SIM card".
26. Once fraudsters have these numbers, they can intercept two-factor authentication codes, reset passwords, and access bank accounts, email, and social media.³¹
27. The consequences of SIM swap fraud are devastating. In June 2023, Toronto Police arrested 10 people and laid 108 charges in Project Disrupt—a major SIM swap investigation. Combined losses exceeded \$1 million.³² The CRTC has also recognized the seriousness of SIM swap fraud. In 2020 and 2023 its staff issued letters requiring mobile carriers to track and report data on unauthorized SIM swaps and port-outs. These letters acknowledge that SIM swapping is a significant threat to consumers. TELUS' solution?: not to invest more heavily in system security but to impose device-locking on consumers.
28. Device-locking is an inefficient approach to SIM swap fraud because the hardware lock does not prevent fraudsters from convincing TELUS representatives to transfer numbers. Imposing an external hardware block does not correct or resolve WSPs' internal authentication problems, but instead penalizes all consumers for its security failures. Rather than minimally impairing consumers, TELUS wants the CRTC to empower all WSPs to impose device-locking, a disproportionate response to inadequate business security practices which fails the "minimal impairment" test.
29. The Commission should issue an RFI requesting data about Sim Swap issues from all WSPs and publish this information on an aggregated basis (to protect the interests of individual companies).

³¹ Telus, [Understanding SIM Swap fraud and how to protect yourself](#).

³² Ron Fanfair, Toronto Police Service ["Project Disrupt Leads to Arrests and Charges"](#), (1 August 2024).

30. FRPC considers that TELUS – not the public – bore the onus to provide evidence to support its application and has not done so. The CRTC should therefore deny its application.

III. Six reasons to deny TELUS' device-locking proposals

31. FRPC opposes TELUS application for several other reasons beyond stale or absent evidence. Most importantly, TELUS has not provided relevant – and in particular, up-to-date – facts to support its outlandish claims that its employees and potential customers are at risk ... from rising supply-chain theft over which the customers most directly affected by device-locking have no control.
32. Second, TELUS has not explained how its thinly veiled attempt to limit competition in the wireless sector by locking unwilling customers to the corporate bosoms of Canada's WSPs for two months meets Parliament's desire that Canada's telecommunications policy "respond to the economic and social requirements of users" in the telecommunications system.³³
33. Third, TELUS has not explained how locking new subscribers' devices for three months *strengthens* "the position of consumers in their relationships with service providers, including by ... taking measures to ensure that consumers can promptly, affordably and easily cancel, downgrade, transfer or otherwise change their services" as required by Cabinet's February 2023 *Direction to the CRTC on a Renewed Approach to Telecommunications Policy*.³⁴
34. These are the most important reasons for the Commission to reject TELUS application – but there are several others that merit consideration.

A. The CRTC rejected Bell's device-locking proposal eight months ago

35. The Commission's letter to Bell Canada dated November 28, 2025 already decided this matter, stating that device-locking practices are an unnecessary and disproportionate response to Bell's concern. The CRTC found that:

Bell has not demonstrated that the practice of locking cellphones for up to 60 days after purchase is a necessary and proportionate response in this case. Specifically, Bell has not demonstrated that this practice is effective, nor that it has exhausted alternative solutions that comply with the Wireless Code.³⁵

³³ *Telecommunications Act*, s. 7(h).

³⁴ *Order Issuing a Direction to the CRTC on a Renewed Approach to Telecommunications Policy*, [SOR/2023-23, P.C. 2023-110 \(2023-02-9\)](#).

³⁵ *Supra* note 1

36. The Commission explicitly stated that “locking cellphones is not in the best interest of consumers” and expressed concern that Bell “opted to disregard a key consumer protection outlined in the Code”.³⁶ This decision is final, rather than interim.
37. TELUS's May 2026 application attempts to relitigate the arguments that the Commission rejected in November 2025. It has not provided new evidence to overcome the Commission's finding in that decision, it has not demonstrated that a 60-day lock is effective and it has not exhausted alternative solutions. The onus in this application rests on TELUS to provide this objective evidence, and it has failed to do so.
38. The Commission should apply the standard in the Bell matter to TELUS and deny its request for interim relief: granting TELUS' request would effectively reverse the CRTC's recent, well-reasoned decision without evidence of the material change in circumstances or evidence such a reversal requires. Rather than granting TELUS request, the CRTC should ensure that all WSPs are meeting the *Codes'* requirements.

B. Device-locking nullifies the 15-day trial period

39. Under Section G of the Wireless Code, consumers are legally entitled to a 15-day trial period “to enable the customer to determine whether the service meets their needs”.³⁷ This is a fundamental consumer protection is fundamental, especially for members of accessibility communities.
40. In rural, topographically complex regions such as the Gatineau hills (as described in Bell's Part 1 forbearance file for Quebec, Manitoba and Atlantic Canada),³⁸ carrier coverage maps claiming “Full 5G” frequently fail at ground level due to mountains, cliffs, dense foliage, and valleys. Consumers who rely on these maps may wind up contracting for services that cannot meet their needs.
41. Consumers must have the ability to compare networks within the 15-day window. Making an informed decision within the 15-day window requires insertion of the SIM card of the consumers' WSP to compare signal strength and data performance.
42. A 60-day device block restricts informed consent because consumers cannot then check coverage using the WSP's competitor's SIM, nullifying their statutory right to withdraw from the contract.

³⁶ *Supra* note 1

³⁷ CRTC Wireless Code, “[Mobile service trial period](#)”.

³⁸ [Application for forbearance from the regulation of residential local exchange services in Atlantic Canada](#); [Application for forbearance from the regulation of residential local exchange services in Manitoba](#); [Application for forbearance from the regulation of residential local exchange services in Ontario and Quebec](#).

43. FRPC opposes TELUS' application. If, however, the CRTC decides to grant it on an interim basis, the Commission must then extend the trial period to the device-locking period and an additional 15 days: 75 days in total.

C. Device-locking unlikely to reduce or prevent theft

44. As noted earlier, TELUS argues that device-locking is needed to reduce or prevent violent theft. As **Error! Reference source not found.** shows, WSPs have taken steps to protect their staff and their stores. Walk-in retail audits of TELUS competitors such as Rogers found prominent consumer notifications detailing the use of time-activated smart safes and delayed next-day fulfillment protocols for high-value hardware including wireless devices.

Figure 2 Rogers' retail outlet in Ottawa (July 2026)



45. These measures effectively mitigate retail theft without removing the protections granted by consumers by the Commission, and without requiring new subscribers to give up hard-won consumer rights established to protect their interests
46. It is important to note, however, that even more recent reports about device theft establish that device-locking would not stop such theft. This is in part because when a carrier-locked phone is stolen, normal voice calls, cell data and SMS texting are blocked – but systems that function over WiFi such as apps, browsing, social media, steaming services and other voice-call apps continue to function. A locked device still provides partial functions.
47. The partial functioning of locked devices helps to explain why, as Appendix 2 demonstrates, unlocked and locked devices alike will still be subject to theft. Such theft

is driven by common street-level crimes such as pickpocketing, distraction theft, and break-ins. In distraction thefts, criminals divert a victim's attention to steal valuables like cell phones, cash, or jewelry; police noted that thieves “often target vulnerable populations, like the elderly”, and rely on “kindness, politeness and trust”.³⁹

48. News reports in mid-2025 and early 2026 warned of “pickpockets targeting cellphones at public festivals”,⁴⁰ with CityNews reporting that police were urging vigilance as summer festivals approached. Earlier this year CP24 reported on a “surge in cellphone thefts in Toronto”, linking it to a broader trend of street-level crime.⁴¹ Police investigated two alleged cellphone pickpockets caught at the Rebel nightclub,⁴² highlighting the organized nature of street-level theft.⁴³
49. TELUS’ proposed 60-day device lock cannot reduce these forms of theft. A pickpocket stealing a phone from a pocket or a bag, or a thief using distraction technique will not be deterred by device locks because stolen devices are often not resold as functioning phones. They are “strip-mined” for high-value replacement parts – screens, cameras, logic boards, and batteries – that are then sold on global grey markets. Whether three or twelve months long, device locks will not stop devices from being stolen for their parts. They simply recreate the barriers and disadvantages the CRTC eliminated in 2017.
50. FRPC also understands that device manufacturers such as Apple have cloud-based activation locks (e.g., MDM/Activation Lock) that can render a stolen device useless for resale. Both Apple and Android platforms use cloud-linked security tokens to enforce these locks at the motherboard level, making a stolen device impossible to reactivate after a factory reset.
51. TELUS, meanwhile, notes that the alleged surge in mobile phone thefts – which happened seven years ago – “has escalated beyond storefronts into the supply chain itself” (¶13). It adds that “no segment of the device distribution network is safe from these increasingly sophisticated criminal actors.”
52. In other words, effective theft mitigation belongs at the inventory level, not at the level of the consumer. If technology permits automated point-of-sale whitelisting, a post-purchase 60-day lock serves no anti-theft function for a phone that has safely left the store. TELUS should not be permitted to substitute a blunt, anti-consumer shortcut for standard physical internal security infrastructure and proper internal fraud prevention.

³⁹ Appendix 1: 8 June 2026 “Distraction thefts are on the rise in Toronto, police urge vigilance as FIFA approaches”.

⁴⁰ Appendix 1: 26 June 2025, “Toronto police seeing increased reports of pickpockets targeting cellphones at public festivals”

⁴¹ Appendix 1: 25 February 2026, “What’s behind the surge in cellphone thefts in Toronto”.

⁴² Appendix 1: 17 February 2026, “Toronto police investigating after 2 alleged cellphone pickpockets caught at Rebel nightclub”.

⁴³ Appendix 1: 26 June 2025, “Toronto police warn of rising cell phone thefts by pickpockets”.

WSPs whose supply chains have been breached should not be permitted to push the costs of these breaches onto consumers (by using device-locking to discourage subscription switching).

53. Rather than tackling supply-chain and distribution-network crime, however, TELUS instead demands that the Commission punish new subscribers by allowing all WSPs to lock the devices they are buying or renting.

D. Device-locking converts owned devices into rentals

54. Smartphone purchases today are a type of credit-financed property transfer. A purchaser (consumer) is the device's legal owners.
55. Investigative evidence from CBC News and independent telecom journals like *iPhone in Canada* has shown that when sophisticated delivery scams or "inside job" data leaks occur, carriers continue to hold consumers entirely liable for the hardware cost. Rogers stated that "Once a device is delivered, whatever happens with it afterward is the customer's responsibility". In mid-July *iPhone in Canada* reported the case of scammers who had obtained the exact delivery details of a new device, the customer's contract information and knew precisely when the device was delivered: this points to WSP system vulnerabilities or data leaks within the WSPs' telecom ecosystem. Device-locking in such cases achieves nothing because the criminals already have the device: they are exporting it, strip-mining it for high-value parts or waiting out the 60 days.
56. The Forum opposes TELUS' application because one result is to cushion and protect WSPs from gaps in their internal security systems and safeguards, while transferring responsibility for these problems to consumers.
57. If, however, the CRTC decides to grant WSPs effective control over customers' devices through device blocking on an interim basis, the CRTC should then also transfer liability for devices stolen through fraud from the customer to the WSP. Risks should then be shared between both parties to the contract, rather than be unilaterally placed on consumers.

E. Device-locking puts Canadians at risk

58. Section 7 of the *Telecommunications Act* requires regulation that facilitates "the orderly development of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada" and that responds "to the economic and social requirements of users." Device-locking practices contravene these requirements by reducing consumer safety.

1. A Locked Phone Undermines the "9-1-1 Safety Net"

59. Some parties may argue that device-locking does not compromise public safety because any phone, locked or not, can dial 9-1-1. This argument does not reflect the way that Canada's telecommunications system operates.
60. On July 22, 2026, a province-wide 9-1-1 outage occurred in Manitoba due to a fibre cut.⁴⁴ During this outage, residents were instructed to call 10-digit emergency numbers if 9-1-1 failed. The problem for some residents was that locked devices that are effectively stranded on a non-functioning network cannot place that call and also will not switch to a competitor's network to place the call. In some areas smaller communities use alternatives in addition to or as a substitute for Canada's National Public Alerting System (as discussed in the CRTC's 2025 Emergency Alerting consultation⁴⁵).
61. It is true that in the wake of several major national network outages, Canadian telecommunications companies signed a formal [Memorandum of Understanding on Telecommunications Reliability](#), promising mutual assistance and Emergency Roaming during mass disasters. Yet emergency roaming protocols are designed for rare, mass network failures, rather than daily localized dead zones. Device-locking of mobile phone hardware for 60 days creates a new and important point of failure at the level of the user who lives in those areas. By compromising a consumer's ability to access these lifelines device-locking is contrary to the public interest.

2. Locked devices block non-9-1-1 calls for help

62. The tragic Switzer case also shows that a carrier's network can fail for a specific user or in a specific location, leaving users without a communication lifeline.⁴⁶ While a locked phone can dial 9-1-1 on any network (as required by law), it *cannot* receive incoming wellness checks from family or non-emergency support from local utilities or roadside assistance if the primary network is dark. It cannot dial emergency services in areas without 9-1-1 access. It cannot dial emergency services when emergency services are affected due to a province-wide outage like what occurred in Manitoba. Emergency service override only works for outgoing calls and only in specific circumstances, as tragically illustrated by the Switzer case.
63. Public safety is in any event not limited to making 9-1-1 calls. Mobile calls placed by users who need to contact local utilities about downed power lines, call a local tow truck during a winter storm or report a non-injury accident to local police are not routed

⁴⁴ CTV News Winnipeg, [911 outage resolved in Manitoba: Bell](#), (22 July 2026).

⁴⁵ CRTC *Call for comments - Improving the public alerting system*, [BTNoC 2025-180](#).

⁴⁶ CTV, ["Telus alleges man's death during 911 outage 'caused or contributed' by his own negligence: lawsuit"](#), (2 May 2026).

through an emergency service override. In such cases device-locked users are cut off from non-9-1-1 help.

64. Canadians need to be able to receive life-saving emergency alerts during wildfires or tornadoes. A 60-day lock may actively endanger people living in or visiting rural areas as well as First Nations residents by denying them access to the multi-network communication lifeline that unlocked devices provide.

F. Device-locking introduces biometric identity authentication

65. TELUS's application includes, at paragraph 124(c), a casual reference to a proposed fraud-mitigation safeguard that would permit service providers to validate customers through "biometric identity authentication" when processing early unlocking requests. Perhaps the idea is that biometric-identification requirements would help WSPs to deal with SIM swapping by fraudsters. If TELUS' customer authentication processes is malfunctioning it should correct its problems by strengthening its internal security and authentication systems, rather than proposing to acquire biometric information from consumers.
66. In any event, the nature of the biometric information involved is not clearly described. Does TELUS intend to solicit a sample of skin tissue? Blood? Hair? Fingerprints? Retinal scans?
67. The possibilities seem as broad as their potential uses, and require more clarity than TELUS has provided for an interim application in a telecom proceeding. The lack of detail is especially surprising, given that TELUS is "[s]caling [its] global growth engines: Health, Digital and Agriculture & Consumer Goods".⁴⁷ Among other lines of business it has developed TELUS Health, which "operates data centres and uses cloud-centric infrastructure to collect and manage data on behalf of customers, including sensitive personal health information, which may move across [its] interconnected operational and business support systems and networks."⁴⁸ In September 2025 TELUS

... announced a partnership with League, to power its comprehensive AI-driven health platform utilizing our Sovereign AI Factory. League is a leading healthcare consumer experience platform, powered by AI. The League platform will leverage our sovereign infrastructure to physically store sensitive healthcare data within Canada's borders, supporting a key priority for the development of secure, privacy-compliant and sovereign AI, while enabling advanced research and development of unique Canadian-centric models.⁴⁹

⁴⁷ TELUS, [2025 TELUS Annual Report](#).

⁴⁸ TELUS, [2025 TELUS Annual Report](#), at 85.

⁴⁹ TELUS, [2025 TELUS Annual Report](#), at 16.

68. To the best of FRPC's knowledge, biometric-identification requirements in the context of wireless-device subscriptions are new, as are the approach that should be taken to meet Parliament's telecommunications policy objectives. FRPC strongly opposes the imposition of such requirements on any basis, including with respect to this interim application's request.

1. A new barrier

69. Biometric-identification requirements are unnecessary to 'validate' customers who are seeking 'early unlocking' or any other type of unlocking. It must be assumed that WSPs have already undertaken their own due diligence with respect to new customers just prior to the point of sale, immediately before the customers and the WSPs formed their contract. These are checks that should be performed at the time of purchase, not retroactively imposed on consumers who have already been vetted and approved for financing. The CRTC should prohibit WSPs from seeking or obtaining yet more customer information after that point.

70. If TELUS requires biometric validation to confirm identity (glancing at a card), it should be performed at the point of sale—before the device leaves the store—not days, weeks or months later when consumers seek to exercise their right to switch providers.

2. A significant invasion of privacy

71. TELUS' proposal for biometric-identification requirements goes well beyond the scope of a simple device lock. Biometric data is a uniquely sensitive category of personal information and its use by a telecommunications provider is a major step that demands thorough public scrutiny. It may adversely affect seniors living in Quebec, as many neither have nor require photo ID (RAMQ health insurance cards, for instance, do not necessarily include a photo for all residents).⁵⁰

72. Yet the Commission's staff has previously informed a consumer that privacy-related issues, specifically "whether business practices involving Plaid or similar services infringe upon customers' privacy",⁵¹ are considered "out of scope" for the broader consumer protection harmonization proceeding (BTNOC 2026-134). The CRTC's [24 July 2026 letter](#) closed his Part 1 Application with respect to privacy issues.

73. Adding biometric-identification requirements creates a new barrier to obtaining wireless telecommunications service that is neither necessary nor proportionate to the stated goal of fraud prevention. Such requirements have the perverse effect, however,

⁵⁰ RAMQ, [Health Insurance Card](#).

⁵¹ Émile Arsalane, [Part 1 Application Regarding Conditional "Discounts" for Automated Bank Debits, Payment Processing Penalties, Third-Party Data Aggregators, Connection Fees, Post-Cancellation e-Statement Charges, and Ancillary Fees in the 2025 Retail Wireless Market](#), (18 December 2025).

of normalizing a significant intrusion on Canadians' right to privacy. Where Mr. Arsalane's request to address privacy concerns was not even granted process, TELUS has been granted *carte blanche* to seek reductions in consumers' right to privacy: this approach to process implies the existence of a two-tier system where carriers may introduce privacy-impacting practices while members of the public are barred from challenging the practices.

74. TELUS proposal to gather biometric data butts up against Canadians' *Charter* right to privacy. But it also enables the company to develop a new business stream by harvesting and selling the data. Even if the data were anonymized, the simple fact is that Canadians had no meaningful way of opposing this request to breach their privacy and possibly sell their core data, because it has been presented in a Part 1 application that, as 'regulars' in the CRTC's are only too aware, attract very little public attention.

IV. Concerns about the impact of granting TELUS' interim-relief application ...

A. Relying on existing procedural rights may trigger device-locking

75. TELUS states at paragraph 116 that automatic unlocking will occur after 60 days, provided that the associated account is in good standing and not subject to indicators of fraud or misuse. These conditions include:
- An active account that does not have an outstanding past-due balance or payment arrears, and the first invoice has been paid in full;
 - the device' not being blocked as fraudulent, or reported lost or stolen;
 - evidence of normal customer use; and
 - the account has not been flagged for suspected fraud, identity misuse, or payment reversals.
76. Suppose, however, that a mismatch occurs between what customers were promised at the point of sale and what the WSP later delivers – an issue known to and documented by the CCTS – whether due to fees' being different, plan characteristics' being different, or other discrepancies. According to the CCTS statistics, it is not abnormal for WSPs to fail to respond to customers' calls about such matters, for days. The onus falls on the customer to navigate these delays – an unreasonable burden, particularly when time-sensitive issues such as travel or relocation are involved.
77. After two unsuccessful approaches to their WSP consumers may approach the CCTS to seek resolution of their problem. They also have the right not to pay the difference when prices are disputed until the CCTS has concluded its review.
78. Yet the CCTS can take many months to address a complaint. According to TELUS (¶116), these accounts would not be "in good standing" (¶116). The subscriber would therefore be ineligible to be unlocked even though "fraud" is not involved.

79. In other words, approving TELUS' interim application means that consumers would be penalized for exercising their right to dispute billing errors.

B. Device-locking as boundary testing

80. TELUS's public statements regarding unilateral deployment dates for locking mechanisms (¶¶13, 112, and 175 of its application) prompted an explicit CRTC Staff Warning Letter on 8 July 2026 and indicate a troubling willingness to test the boundaries of the *Wireless Code*.
81. The Commission's letter reminded TELUS that "WSPs are responsible for remaining compliant with the *Wireless Code* at all times" and that "the current rules in the *Wireless Code* requiring WSPs to provide customers with unlocked devices remain in effect unless and until the Commission makes an express decision otherwise".⁵²
82. TELUS's stated intention to implement the lock on July 30, 2026, before the Commission has even ruled on the interim relief, directly challenges the CRTC's authority, and reflects the Bell "fait accompli" approach that the Commission criticized in its November 2025 letter.
83. If the Commission permits private commercial entities to alter consumer property rights through interim Part 1 applications, the regulatory authority of the *Wireless Code* will effectively collapse.

C. Interim steps may lead to permanent changes

84. The Forum is also concerned that TELUS's interim request (in this proceeding) for a 60-day lock is simply a first step. As demonstrated by the Verizon filing,⁵³ extensively copied, the U.S. carrier used the same "fraud and theft" justification to secure a 60-day waiver, only to later admit it was insufficient and request a much longer lock of 3 to 6 months or more. TELUS is employing the identical playbook.
85. Granting this interim relief would open the door to further requests for extended locking periods—3 months, 6 months, or potentially for the entire duration of the device financing term. The true objective is not crime prevention but to permanently tether consumers to TELUS's network and to create barriers to other carriers.

⁵² CRTC, [Subject: TELUS – Part 1 Application to implement a 60-day device lock on a temporary and permanent basis](#), Telecom - Staff Letter addressed to Stephen Schmidt (TELUS Communications Inc.), (Gatineau, 26 July 2026).

⁵³ Verizon, *In the Matter of Verizon Request for Waiver, Regarding the Commission's Ban on Locking Handsets for C-Block Licensees, Request for Waiver* (19 May 2025); noted in <https://docs.fcc.gov/public/attachments/DA-25-490A1.pdf>.

V. Conclusions and recommendations

86. TELUS should be commended for its concern about its employees' safety and device theft. The solution to concerns about safety is for TELUS to employ security guards in its retail outlets;⁵⁴ a partial solution for device theft is to tighten the companies' supply-chain systems.
87. The CRTC should deny TELUS' application, however, because allowing all WSPs to begin device-locking will limit consumers' rights to privacy (by permitting the capture of their biometric information), to enjoy their property, to ensure they receive the coverage they have been promised or to have ready access to calls made for emergency purposes.
88. The Commission should also deny TELUS application because device-locking is not rationally connected to reducing violent crime at retail outlets, or to preventing or stopping opportunistic pickpocketing or distraction-based theft. Nor has TELUS explained why alternatives that minimally affect consumers' rights, such as safes and the National IMEI Blacklist, are insufficient to secure and protect device inventory.
89. Consumers do not benefit from the reduction of their rights, the current competitive market in telecommunications will not benefit from the re-imposition of old barriers and people living in or visiting rural areas of Canada will not benefit from loss of ready access to emergency services due to the technical limitations of device-locking. Who does benefit, really, in the scenario proposed by TELUS?
- A. **Effective and less restrictive alternatives exist, including Rogers' "smart safe"**
90. TELUS presents a false dichotomy to the Commission: that it must either restrict consumer hardware for 60 days or leave retail staff vulnerable to theft. Alternatives to device unlocking exist, however, so that the heaviest practical and financial burden need not fall on innocent customers. Deterring professional criminal activity falls to businesses such as TELUS. The company itself noted that the alleged surge in mobile phone thefts – which happened seven years ago – “has escalated beyond storefronts into the supply chain itself” (¶13). It added that “no segment of the device distribution network is safe from these increasingly sophisticated criminal actors.”
91. Rather than tackling supply-chain and distribution-network crime, however, TELUS instead demands that the Commission punish new subscribers by allowing all WSPs to lock the devices they are buying or renting.

⁵⁴

Whose expense will be deductible from the companies' taxable income.

B. Recommendations

92. FRPC recommends that the CRTC deny TELUS's application for interim relief to implement a 60-day carrier lock, consistent with its November 28, 2025, ruling on Bell's similar practice.
93. If the CRTC decides to grant any form of TELUS' proposal for device locking, it should in the alternative
- Mandate that any anti-theft locking mechanism be automatically and instantly deactivated via Point-of-Sale Whitelisting the moment a consumer transaction is completed.
 - Require that the 15-day trial period be extended to at least 75 days to account for the 60-day lock, ensuring consumers have a meaningful opportunity to test network service.
 - Require carriers to offer a clear, enforceable "Anti-Theft Guarantee" where the carrier assumes liability for fraud or theft during the lock period, shifting the risk back to them where it belongs, and
 - Require carriers to guarantee seamless access to **all** emergency and non-emergency communication channels—including 10-digit emergency numbers, the Alert Ready system, and incoming voice communications—during the device-locking period and when services may be down for that particular provider.
94. The CRTC should also
- a. Clarify the scope of this proceeding to expressly include consideration of whether TELUS's proposed use of biometric identity authentication (paragraph 124(c) of the Application) is a "necessary and proportionate" measure, or in the alternative, issue a direction that no reliance will be placed on paragraph 124(c) in determining whether the interim relief should be granted,
 - b. Issue a public warning that any carrier implementing a device lock without express Commission authorization will be subject to enforcement action, including Administrative Monetary Penalties (AMPs), consistent with the Commission's warning to Bell, and
 - c. Order carriers to utilize less restrictive means, such as the National IMEI Blacklist and physical retail security infrastructure (e.g., time-activated smart safes), to resolve corporate shrinkage issues without penalizing consumer property rights.
95. The Commission has already ruled that a 60-day lock is not in the best interest of consumers and that not evidence supports its necessity or proportionality. TELUS's application offers no new evidence to overcome this precedent. The company's application for interim relief should be denied, and it should be directed to pursue any



legitimate security concerns through the proper regulatory channels, including the comprehensive 2026-134 *Harmonized Codes* proceeding.



Appendices

Appendix 1	CRTC's 8 July 2026 Staff Letter to TELUS	1
Appendix 2	Theft of cellphone devices: pickpocketing	3



Appendix 1 CRTC's 8 July 2026 Staff Letter to TELUS

[Telecom - Staff Letter addressed to Stephen Schmidt \(TELUS Communications Inc.\)](#)

[Gatineau, 8 July 2026](#)

Reference: 8665-T66-202603464

zoom

TELUS Part 1 application posted on 8 July 2026

BY EMAIL

Stephen Schmidt

Vice-President – Telecom Policy & Chief Regulatory Legal Counsel

TELUS Communications Inc.

regulatory.affairs@telus.com

Subject: TELUS – Part 1 Application to implement a 60-day device lock on a temporary and permanent basis

Dear Stephen Schmidt,

On 22 May 2026, TELUS Communications Inc. (TELUS) filed a Part 1 Application seeking temporary and permanent authorization for wireless service providers (WSPs) to implement a 60-day device lock on new subsidized or financed devices. TELUS requested that the temporary authorization for the 60-day device lock take effect 60 days from the date of its application. It also requested that the permanent authorization for the 60-day device lock be made permanent through formal amendments to the Wireless Code.

By means of this letter, Commission staff is informing you that TELUS' Part 1 application has been posted on the Commission's website.

At paragraphs 13, 112, and 175 of its application, TELUS indicates that it intends to implement a temporary 60-day device lock on all new device activations on 30 July 2026. TELUS submits that this measure is a necessary and immediate response to protect TELUS' employees, customers, and the integrity of its network while its application is under consideration. Although Commission staff acknowledges TELUS' submissions on safety and security, staff reminds TELUS that WSPs are responsible for remaining compliant with the Wireless Code at all times. Therefore, the current rules in the Wireless Code requiring WSPs to provide customers with unlocked devices remain in effect unless and until the Commission makes an express decision otherwise.

In this regard, the interim relief portion of TELUS' application, which requests a temporary authorization to implement a 60-day device lock on all new device activations, will be considered on the following basis:

Interested persons may submit comments limited to the interim relief requested in TELUS' application by 28 July 2026.

TELUS may submit a reply by 4 August 2026.

As for the request to amend the requirements set out in the Wireless Code, Commission staff notes that the ongoing Harmonizing the consumer protection codes, Broadcasting and Telecom Notice of Consultation CRTC 2026-134, would be the appropriate forum for parties to submit suggestions to amend this consumer protection, as other, similar consumer protections that are already being considered in that proceeding. As such, Commission staff invites TELUS as well as any other interested parties to submit their comments on TELUS' proposal for permanent authorization in that proceeding by no later than 11 August 2026.

A copy of this letter will be posted on the Commission's website.

Sincerely,

Nanao Kachi



Director, Social and Consumer Policy, CRTC,
cc: Keldon Bester, CAMP, keldon@antimonopoly.ca
Tahira Dawood, PIAC, tdawood@piac.ca
Monica Auer, FRPC, execdir@frpc.net
bell.regulatory@bell.ca;
geoff@brooketel.ca;
Regulatory@brucetelecom.com;
Regulatory.Matters@corp.eastlink.ca;
regulatory@corp.wightman.ca;
martha.facey@execulink.com;
a.lawrence@hay.net;
ryan.mcclinchey@hurontel.on.ca;
regulatory@icewireless.com;
regulatory@iristel.com;
knaylor@mornington.ca;
lhallahan@mornington.ca;
regulatory@quadro.net;
regaffairs@quebecor.com;
melanie.cardin@quebecor.com;
rwi_gr@rci.rogers.com;
document.control@sasktel.com;
richard.biron@sogetel.com;
stephen.scofich@tbaytel.com;
regulatory@tccmail.ca;
reglementa@telebec.com;
regulatory.affairs@telus.com;
scott_laird@ztarmobile.com;



Appendix 2 Theft of cellphone devices: pickpocketing

Reported thefts, and types of thefts (The rise of theft since pre-pandemic times that Telus cites):

1. Jun 08, 2026, Distraction thefts are on the rise in Toronto, police urge vigilance as FIFA approaches

<https://www.cbc.ca/news/canada/toronto/police-warn-distraction-thefts-up-fifa-approaching-9.7227447>

2. Feb 25, 2026, What's behind the surge in cellphone thefts in Toronto

<https://www.cp24.com/local/toronto/2026/02/26/whats-behind-the-surge-in-cellphone-thefts-in-toronto/>

3. June 26, 2025, Toronto police seeing increased reports of pickpockets targeting cellphones at public festivals

<https://www.ctvnews.ca/toronto/article/toronto-police-seeing-increased-reports-of-pickpockets-targeting-cellphones-at-public-festivals/>

4. June 26, 2025, Toronto police warn of rising cell phone thefts by pickpockets

<https://toronto.citynews.ca/2025/06/26/toronto-cell-phone-thefts-summer-festivals/>

5. Feb 17, 2026, Toronto police investigating after 2 alleged cellphone pickpockets caught at Rebel nightclub

<https://www.ctvnews.ca/toronto/article/toronto-police-investigating-after-2-alleged-cellphone-pickpockets-caught-at-rebel-nightclub/>

6. Feb 25, 2025, CTV YOUTUBE Video:

How criminals are making big money from small-time cellphone thefts

https://www.youtube.com/watch?v=oiyllvRRz_8

or

https://youtu.be/oiyllvRRz_8



Part 1 Application 8665-T66-202603464 (11 June 2026)

FRPC Intervention (28 July 2026)

Appendices, page 4 of 1
