TELUS – PART 1 APPLICATION TO IMPLEMENT A 60-DAY DEVICE LOCK ON A TEMPORARY AND PERMANENT BASIS

COMMENTS

OF

CANADIAN TELECOMMUNICATIONS ASSOCIATION

28 JULY 2026

Introduction and Executive Summary

1. The Canadian Telecommunications Association ("CTA") provides these comments in support for TELUS Communications Inc. ("TELUS") request for interim relief which requests a temporary authorization for all wireless service providers to implement a 60-day device lock on all new device activations.

2. Pursuant to the procedure set out by the Commission in its letter of July 8, 2026, CTA's comments are directed solely to TELUS' request for interim relief. CTA will provide its comments regarding TELUS' request for permanent authorization for a 60-day device lock in its intervention to Broadcasting and Telecom Notice of Consultation CRTC 2026-134.

3. CTA's members provide wireless services to Canadian wireless subscribers and have extensive experience preventing, detecting and responding to device theft, subscription fraud and identity-related crime. CTA therefore offers the Commission a sector-wide perspective on why the requested interim relief should be granted.

4. CTA agrees with TELUS' submissions respecting the applicable legal test governing requests for interim relief. Rather than repeating those submissions, and without taking a position at this time on whether the Wireless Code, properly interpreted, already permits a 60-day device lock, CTA's comments focus on the broader public interest considerations that strongly support the exercise of the Commission's discretion to grant the requested interim relief.

5. The evidence cited in TELUS' application demonstrates that the risk environment surrounding wireless device theft and subscription fraud has changed materially since the Commission last considered device unlocking requirements. Consistent with the GSMA's recent assessment that mobile device theft is becoming a global safety crisis, wireless service providers have invested heavily in a broad range of fraud and theft prevention measures, but these measures, while important, are not sufficient on their own to address the evolving threat environment.

6. The interim relief requested by TELUS represents a measured and proportionate response to a significant and growing public interest problem. It should not be viewed as replacing existing fraud prevention initiatives or diminishing the importance of the Wireless Code's consumer protection objectives. Rather, it represents a targeted enhancement to the industry's existing anti-fraud measures while the Commission completes its consideration of the application for permanent authorization to implement a 60-day device lock.

7. CTA further supports TELUS' request that any interim relief granted by the Commission apply uniformly to all wireless service providers.

Existing Fraud-Prevention Measures Cannot Fully Address the Current Threat Environment

8. Canadian wireless service providers have invested significantly in measures to prevent and detect device theft, subscription fraud and identity-related crime. Those measures include fraud detection systems, enhanced customer identity verification processes, employee training, strengthened retail security, collaboration with financial institutions and law enforcement agencies, and participation in international initiatives intended to reduce the market for stolen devices.

9. CTA has itself played a role in these efforts. CTA hosts the Device Check Canada website,[1] which enables consumers to check before purchasing a pre-owned device whether a mobile device is listed in the GSMA International Mobile Equipment Identity ("IMEI") database as being reported lost or stolen.

10. These investments remain an essential component of Canada's anti-fraud framework. However, as the evidence filed by TELUS demonstrates, they are not, on their own, sufficient to address the significantly changed fraud and theft environment now facing the industry.

11. For example, while investments in retail security have helped deter certain forms of theft and improve employee safety, they cannot prevent subscription fraud and other schemes involving fraudulently obtained devices. Similarly, fraud detection systems and customer authentication processes continue to evolve, but so too do the techniques used by increasingly sophisticated criminal organizations to immediately activate fraudulently obtained devices before wireless service providers can take steps to address the activity. A temporary device lock addresses this specific vulnerability by removing the incentive for these evolved criminal techniques.

12. Likewise, while initiatives such as DeviceCheck play an important role in reducing the domestic market for stolen devices, they have inherent limitations. As TELUS explains in its application, participation in the GSMA blacklist remains voluntary internationally, allowing sophisticated criminal organizations to export stolen Canadian devices to jurisdictions where blacklist queries are not made or where enforcement is inconsistent, thereby preserving the resale value of those devices for such organizations. Moreover, device blacklisting generally occurs only after a device

[1] https://www.devicecheck.ca/

has been reported as stolen or fraudulently obtained and therefore does not materially reduce its immediate value during the critical initial days after it has been acquired.

13. Existing fraud prevention measures and temporary device locking therefore serve different, but complementary, purposes. Existing measures focus on detecting fraud, protecting customers and employees, and limiting the use of stolen devices after they have been identified. Temporary device locking addresses a different vulnerability by reducing the immediate utility and resale value of a fraudulently obtained device during the period in which the risk of monetization is greatest.

14. The requested interim relief is not being requested as a substitute for existing fraud prevention initiatives, but as an additional safeguard. Wireless service providers continue to invest in other tools and measures to combat theft and fraud, but such tools and measures cannot fully address the evolving fraud techniques described in the TELUS application.

Granting Interim Relief is in the Public Interest

14. The Commission adopted the current device unlocking requirements to advance important consumer protection objectives, including facilitating consumer mobility and reducing barriers to switching service providers. Those objectives remain important today and CTA does not suggest otherwise.

15. However, protecting consumers today requires consideration of a broader range and scale of risks than existed when the current unlocking requirements were adopted. As the TELUS application demonstrates, mobile devices have become substantially more valuable,[2] subscription fraud has become increasingly sophisticated, identity theft has become more prevalent, organized criminal activity targeting wireless devices has increased, and advances in artificial intelligence and other technologies have significantly increased both the scale and sophistication of fraud.

16. These developments have fundamentally altered the environment in which the Commission's existing unlocking requirements operate. As governments in Canada and internationally increasingly recognize fraud as a significant public safety and consumer protection issue, the public interest now encompasses not only facilitating

[2] Prices for mobile devices are expected to continue to rise due to shortages in key components. See for example, "Apple.to.Raise.Prices.Due.to.Memory.Chip.Crunch?.Tim.Cook.Says¿The.CEO.tells.the.Journal.in.an.exclusive.interview.that.soaring.costs.make.price.increases›unavoidable"‹?.Wall Street Journal, June 17, 2026. Among other references to higher prices, the article states the following: 'Morgan Stanley estimates a 15% bump for prices of smartphones and PCs in the U.S. this year."

consumer mobility, but also protecting consumers from fraud and theft, improving employee safety, reducing incentives for organized criminal activity and supporting broader efforts to combat fraud.

17. Temporary device locking directly protects consumers. Since a fraudulently obtained device cannot be immediately activated and monetized, temporary locking materially reduces fraudulent takeovers of customer accounts, sparing consumers the disruption, stress, privacy, and identity-related risks associated with such fraud. Protecting consumers from fraud and identity theft in this way is not in tension with their interests, but squarely advances them.[3]

18. The issue before the Commission at this stage of the Part 1 application proceeding is whether the evidentiary record establishes a sufficient basis to justify temporary interim relief while the request for permanent authorization for a 60-day device lock is fully considered.

19. CTA respectfully submits that the evidentiary record not only justifies interim relief but demonstrates that granting such relief is in the public interest. The record establishes a materially changed fraud environment, demonstrates the limitations of existing anti-fraud measures and supports the implementation of a carefully targeted additional safeguard while the Commission undertakes its broader review of the request for permanent authorization for a 60-day device lock. In these circumstances, declining to grant the requested interim relief pending a final determination would unnecessarily prolong exposure to the very harms identified in the application.

The Requested Interim Relief Reflects the Principles of the 2023 Policy Direction

20. The Commission's responsibility is not simply to preserve the existing regulatory framework, but to ensure that its regulatory measures continue to advance the telecommunications policy objectives set out in section 7 of the Telecommunications.Act as technologies, markets and risks evolve. In doing so, the Commission must also have regard to the Governor in Council's 2023 Policy Direction,[4] which directs the Commission to adopt regulatory measures that are efficient, proportionate to their purpose, and informed by evidence.

---

[3] Bell Canada, "Bell's non-compliance with the Wireless Code – Response", 22 December 2025 (Abridged) (Reference: 1011-NOC2016-0293), paragraph 55.
[4] Order Issuing a Direction to the CRTC on a Renewed Approach to Telecommunications Policy (2023 Policy Direction), paragraphs 4 and 6.

21. The 2023 Policy Direction provides an appropriate framework through which to assess the request for interim relief. When viewed through that lens, the requested interim relief represents a balanced and measured response to a materially changed fraud environment while preserving the right of legitimate consumers to easily switch service providers as the Commission's considers the broader request for permanent authorization for a 60-day device lock.

22. The requested interim relief is, first and foremost, evidence based. It responds to substantial evidence demonstrating that the fraud environment surrounding wireless devices has evolved materially since the Commission adopted the current unlocking requirements. The application documents increasing subscription fraud, organized device theft, identity-related crime and the limitations of existing anti-fraud measures. These matters are not unique to TELUS and are being felt across the mobile wireless industry. Pending the Commission's determination of the broader application, that evidence provides a reasonable basis for authorizing temporary relief.

23. Second, the requested interim relief is proportionate to the problem it seeks to address. The application does not seek authority to impose indefinite device locking. Rather, it seeks authorization, on an interim basis, to implement a temporary 60-day device lock during the period that presents the greatest risk of fraud. The proposal therefore targets a specific vulnerability rather than broadly restricting consumers' ability to use their devices as intended.

24. Third, the requested interim relief is efficient because it complements, rather than replaces, the extensive anti-fraud measures already implemented by wireless service providers. As discussed above, providers have invested heavily in fraud detection systems, enhanced identity verification, retail security, employee training, collaboration with law enforcement and device blacklisting initiatives. The requested interim relief simply adds an important targeted safeguard within that existing anti-fraud framework by addressing a vulnerability that those measures cannot fully resolve on their own.

25. The requested relief is also minimally intrusive. The proposed temporary device lock is accompanied by important consumer safeguards, including automatic unlocking at the conclusion of the temporary period, no unlocking fees and the availability of early unlocking in appropriate circumstances. These safeguards ensure that legitimate consumers are not restricted from using their devices as intended, while substantially reducing opportunities for fraud during the period of greatest vulnerability. Furthermore, real world experience suggests that only a very small

proportion of legitimate, non-fraudulent customers seek to switch providers within the first 60 days after acquiring a new device. A temporary device lock therefore does not meaningfully impede consumer mobility.

26. Rather than fundamentally altering the Commission's existing framework, the application for interim relief proposes a carefully calibrated operational measure that addresses a specific, growing, and urgent public interest concern while allowing the Commission to carefully consider the request for permanent authorization to implement a 60-day device lock.

Other Countries Recognize Role of Temporary Device Locks in Combatting Fraud and Theft

39. The Commission is not alone in confronting these issues. Some international telecommunications regulators have reassessed device unlocking policies in light of the significant increase in device theft and subscription fraud experienced in recent years.

40. Of particular significance is the recent decision of the United States Federal Communications Commission ("FCC"), discussed in the TELUS application. The FCC recognized that mandatory unlocking requirements may impair wireless providers' ability to combat fraud and theft and accepted that temporary device locking can serve legitimate public interest objectives.

41. In particular, the FCC determined that the time period of a 60-day locking period to reduce fraud “does not significantly interfere with [the] policy objective” of reducing barriers to changing service providers.[5]

42. The FCC's conclusions are noteworthy because they reflect the assessment of a sophisticated telecommunications regulator confronting many of the same trends now evident in Canada. Its recognition that evolving fraud risks justify reconsideration of unlocking policies demonstrates that protecting consumer ability to switch providers and protecting consumers from fraud are complementary, not competing, regulatory objectives.

43. The TELUS application also identifies other jurisdictions that permit temporary device locking or have reconsidered their approaches in response to increasing fraud and

[5] FCC, Promoting Consumer Choice and Wireless Competition Through Handset Unlocking Requirements and Policies, WT Docket No. 24-186, Summary of “Notice of Proposed Rulemaking, FCC 24-77, adopted 18 July 2024 and released 19 July 2024”, https://www.federalregister.gov/documents/2024/08/08/2024-16642/promoting-consumer-choice-and-wireless-competition-through-handset-unlocking-requirements-and, paragraph 22.

theft. While each jurisdiction has adopted measures appropriate to its own regulatory framework, these developments demonstrate an emerging recognition that unlocking requirements should be calibrated to reflect changing fraud risks rather than treated as immutable.

The Commission Should Grant Interim Relief

44. CTA respectfully submits that the public interest is served by permitting wireless service providers, on an interim basis, to implement a temporary device lock as described in the TELUS Part 1 application. The requested interim relief is evidence-based, efficient, proportionate and minimally intrusive. It builds upon the industry's existing layered anti-fraud framework, preserves the core consumer mobility objectives of the Wireless Code, includes important consumer safeguards and responds to a significant public interest issue affecting consumers, employees and the broader telecommunications ecosystem.

45. CTA further submits that, for the reasons set out in TELUS' Part 1 application, the requested interim relief also satisfies the applicable legal test for granting interim relief. In particular, the application demonstrates that it raises a serious issue to be determined, that the failure to grant interim relief would result in ongoing harm pending the Commission's determination of the application, and that the balance of convenience clearly favours granting the requested relief in light of the significant public interest considerations discussed above.

Any Interim Relief Should Apply Uniformly to All Wireless Service Providers

46. CTA supports TELUS' request that any interim relief granted by the Commission apply uniformly to all wireless service providers subject to the Wireless Code.

47. The issue before the Commission is not unique to any one wireless service provider. The increasing incidence of subscription fraud, device theft and identity-related crime described in the TELUS application reflects broader trends affecting the wireless sector. Likewise, consistent application of interim relief promotes regulatory certainty and provides consumers with clear and consistent expectations regardless of their chosen provider while the Commission considers the application on its merits.

Conclusion

54. The record before the Commission demonstrates that the risk environment surrounding wireless device theft, subscription fraud and identity-related crime has

evolved significantly since the Commission adopted the current device unlocking requirements.

55. Wireless service providers have responded by investing heavily in anti-fraud and anti-theft measures that include fraud detection technologies, enhanced customer authentication, strengthened retail security, collaboration with law enforcement and device blacklisting initiatives. However, as the evidence filed by TELUS demonstrates and the experience of our members confirms, these measures are not sufficient on their own to address the evolving techniques employed by fraudsters and increasingly sophisticated criminal organizations.

56. The requested interim relief represents a targeted measure that addresses a growing and urgent problem. It is temporary, carefully calibrated, evidence-based and accompanied by important consumer safeguards. It therefore reflects the type of efficient, proportionate and evidence based regulatory response contemplated by the 2023 Policy Direction.

57. Importantly, the requested interim relief does not diminish the consumer protections established by the Wireless Code. Rather, it reflects the evolution of those protections in response to increasingly sophisticated fraud, identity theft and organized criminal activity. The proposal preserves the core objective of consumer mobility while introducing a limited safeguard during the period in which fraud risks are greatest.

58. For these reasons, CTA respectfully submits that the Commission should exercise its discretion to grant the requested interim relief and, consistent with TELUS' request, apply that interim relief uniformly to all wireless service providers pending the Commission's determination of the Part 1 application for permanent authorization to implement a 60-day device lock.

*****End of Document*****