cwta Association canadienne des télécommunications sans fil
Canadian Wireless Telecommunications Association acts

ABRIDGED VERSION

February 14, 2020

Mr. Michel Murray
Director, Dispute Resolution & Regulatory Implementation
Telecommunications Sector
Canadian Radio-television and
Telecommunications Commission
Ottawa, ON K1A 0N2

VIA GC KEY

Dear Mr. Murray

Re: CRTC file: 8665-C12-202000280 - Unauthorized Mobile Telephone Number Porting in Canada

1. The Canadian Wireless Telecommunications Association (CWTA) is in receipt of the Canadian Radio-television and Telecommunications Commission's (CRTC) request for information related to *Unauthorized Mobile Telephone Number Porting in Canada*.

2. CWTA is pleased to provide these responses after consulting with members of the Wireless Number Portability (WNP) Council.[1]

3. CWTA requests that the Commission treat certain information contained in the responses below as confidential. The identified responses are filed in confidence pursuant to section 39 of the Telecommunications Act, sections 30-34 of the Rules of Practice and Procedure and section 20 of the Access to Information Act. CWTA and WNP Council members would never publicly disclose details of steps the industry is taking or contemplating taking to prevent unauthorized ports and SIM-swaps other than to the Commission. The information submitted contains detailed fraud prevention measures, and its release would enable fraudsters to better understand the measures implemented by the industry to protect Canadian consumers from fraud, thus circumvent these measures and expose consumers to further harm. CWTA submits that any possible public interest in disclosure of this Information is greatly outweighed by the specific direct harm that would flow to Canadians and the WNP Council members.

BACKGROUND:

4. In 2005, the Commission released Telecom Decision CRTC 2005-72, with the goal to implement wireless number portability in Canada. The aim of this Decision was for number portability to foster competition and allow consumers the ability to switch wireless service providers (WSPs) with minimal delay (i.e. in no longer than 2.5 business hours).

[1] WNP Council members include: Bell, Eastlink, Freedom Mobile, Rogers, SaskTel, Tbaytel, TELUS, and Videotron.

T 613 233 4888 F 613 233 2032 www.cwta.ca
300-80 rue Elgin Street Ottawa, ON K1P 6R2

5. The framework for WNP has been in place since March 2007, allowing Canadian wireless subscribers to successfully "port" their phone numbers via industry developed systems and processes without the requirement for customers to confirm the port with their old WSP. This process proved to be optimal for over a decade.

6. Efficient wireless porting in Canada is premised on cooperative work that occurs at the industry level by the WNP Council. The WNP Council is responsible for the development of industry operational processes and maintenance of the technical specifications necessary for wireless-to-wireless porting. This allows the WNP Council to stay apprised on WNP issues, working collaboratively and with consensus, and to quickly and efficiently adapt to change in an agile manner.

HISTORY OF SIM-RELATED FRAUD:

7. SIM-related fraud is not new, nor is it unique to Canada. SIM-related fraud has long been an issue in Europe and Africa, and in recent years the trend has grown in North America.

8. SIM-related fraud is often financially motivated with fraudsters wishing to gain access to a consumer's banking, cryptocurrency, or other online accounts. It is accomplished by the fraudsters obtaining customer personal information through a variety of means, including social engineering, purchasing customer information from the dark web, or phishing.

9. Unfortunately, it has become easier for fraudsters to take advantage of consumers. Many Canadians inadvertently provide their personal information to fraudsters in innocent ways, such as by posting it on social media websites, or by using "life passwords[2]", which once obtained by fraudsters can be used for a variety of purposes.

10. The use of porting to perpetuate fraudulent activity is another example of fraudsters testing systems to identify weaknesses for exploitation. The wireless industry has taken, and continues to take, steps to protect customers and make it harder for criminals to defraud Canadian wireless subscribers using the porting process.

Question 1: A description of how unauthorized ports are accomplished

11. The motivation for fraudulent WNP activity appears to be malicious in nature.

12. Many organizations, including financial institutions and social media, have implemented Two-Factor Authentication as a security mechanism for their customer accounts. Two-Factor Authentication involves the use of confirmation codes that are sent to a customer's device which then allow the customer to access or make account changes.

13. The porting process has been targeted by fraudsters to serve as a mechanism to defeat this additional security layer.

[2] Life Password is a password that is used by a consumer for logging in to every website and online account.

14. Once fraudsters have the customer's personal information, they can execute a SIM-swap or wireless port and route all text messages and phone calls to their own device. In the instance of Two-Factor Authentication, these new codes are sent to the fraudster's device and they are then able to gain control of the victim's accounts.

15. As WSPs become aware of fraudulent activity and put measures in place to mitigate its occurrence, fraudsters will likely employ new tactics or move their attention to new areas or industries where they think they can identify weaknesses for exploitation.

INFORMATION HARVESTING:

16. The first steps undertaken by a fraudster seeking to defraud Canadians usually include harvesting the personal information of the target. This is done in a variety of ways including but not limited to:
    - Accessing information that is readily or easily available, for example via the target's Social Media presence, or unsecured email accounts. This information while seemingly innocuous on its own has a greater impact when gathered and used together;
    - Social Engineering campaigns aimed at the target encompass many different strategies and techniques, such as e-mail or text message phishing, and change over time. The target inadvertently participates in the data harvesting by providing the fraudster with additional information;
    - Acquiring personal information from the "dark web"; or
    - Buying information from organized criminals (e.g. info that was obtained by criminals through data breaches/hacks).

17. In instances where fraudsters have been successful at socially engineering a WSP's customer service agent, they have often already gathered personal information about the target and use it to impersonate the target, as well as verify or obtain additional details. With this information, the fraudster is authenticated as if they were the customer.

18. Once a consumer's credentials are compromised, they can be used by fraudsters for multiple malicious purposes across multiple industries.

INITIATION OF A FRAUDULENT PORT:

19. By the time the fraudster contacts the new service provider (NSP) they have gathered all necessary information to allow them to successfully pose as the target.

20. When the fraudster contacts the NSP they establish a new account. In most cases, accounts opened as part of fraudulent activity are prepaid accounts.

21. With an account in place, the port is initiated and proceeds using the current industry defined porting processes (refer to Question 3).

CUSTOMER IMPACT:

22. Once the port is completed, the target finds that their device is no longer connected to the network. All calls and texts intended for the target's telephone number are now routed to the fraudster's phone, and the fraudster takes the final steps in accessing the desired information.

PORT REVERSAL:

23. When the target identifies that they can no longer use their service and report this to their WSP, the port is reversed using the porting processes.

Question 2: Available data from the CWTA and its members indicative of the prevalence of unauthorized ports and SIM swapping in Canada, such as the number of instances of each, by wireless carrier, over the last 6 months

24. The requested information is confidential to each WSP and, to the extent available, will be shared in confidence with CRTC directly by each WSP member of the WNP Council.

25. It is important to note that there may be variations between WSPs in how they track such data and what can be provided to the Commission.

Question 3: A description of the information that wireless carriers currently obtain from customers as part of the wireless to wireless number porting process, and how this information is used or verified before a port is permitted

ESTABLISHING AN ACCOUNT:

26. When a customer is porting their number from their Old Service Provider (OSP) it is to acquire service with a NSP while retaining their existing telephone number.

27. To initiate a port request, a customer must first establish an account with the NSP. New accounts may be established online, in store, or through a call centre service representative.

28. When establishing postpaid service, customers are required to provide personal information and consent to a credit check. Personal information may include name, address, and other identifiers required to complete a credit check. Identification is validated through the credit check process.

29. When establishing prepaid service, a credit check is not required. Under the Personal Information Protection and Electronic Documents Act (PIPEDA), organizations must limit collection of personal information to only that which is required for a legitimate business purpose. Since no credit check is completed for a prepaid customer, there is no need to collect name, address, or identification to validate the customer. In keeping with PIPEDA, WSPs do not require the collection of this information.

VALIDATION OF PORT REQUEST:

30. It is the responsibility of the NSP to ensure that it has properly identified the customer initiating the port. The port validation process is part of a fuller order confirmation process.

31. In the validation of a single-line port request, a telephone number is a mandatory requirement and must be included along with at least one of the following data elements:
    - Account Number

- Password /Personal Identification Number (PIN)
- Equipment identifiers such as Equipment Serial Number (ESN) / Mobile Equipment Identifier (MEID) / International Mobile Equipment Identity (IMEI)

32. A port request is then submitted by the NSP using defined industry processes where the required information is processed and validated by the OSP.

33. Where the information is validated, the port proceeds to completion. When not validated, the port request is rejected and sent back to the NSP to action.

Question 4: The information that is exchanged between wireless carriers when a customer is changing wireless carrier

34. A port request requires the exchange of information described in paragraph 31 above.

Question 5: A description of the customer and technical information which gets modified in carriers' databases as a result of a port

35. WSPs have many different databases and systems where some details may be modified as a result of successful port activities.

36. From a technical perspective, on the confirmed due date/time of the port request, the number is activated in the Number Portability Administration Center (NPAC) database. This information is sent to NPAC via the Clearinghouse[3] and identifies that the mobile number has now been moved to the NSP. Since the NSP has also provisioned their switching systems, traffic is now routed to the mobile number that was ported via the NSP's network. As the number no longer routes to the OSP's network for completion, the OSP removes (or reflects the wireless number as ported out) in their switch immediately after the port has occurred. There may also be additional long-distance switch activities that need to be made by both the OSP and NSP.

37. From a customer information perspective, there may be various records or databases that would be updated. The OSP would reflect the wireless number as disconnected/cancelled in their customer information records and ensure that they have stopped billing for it. In instances where a customer no longer has any services with that OSP, the OSP would ensure that the customer's account is cancelled. Cancellation triggers a series of activities that include the issuance of a final bill to the customer, along with the details for any equipment returns (in the case of other bundled services). The NSP would alternatively reflect the wireless number and customer status as active in their systems and commence billing for the wireless service.

[3] WSPs have implemented WNP utilizing a common Service Bureau system. The Service Bureau facilitates the full end-to-end porting process. The Clearinghouse is a component of the Service Bureau that supports connectivity.

Question 6: A detailed description of the measures that the Canadian mobile industry is taking or contemplating to take to prevent unauthorized ports and SIM swapping, including key milestones and timelines

38. CWTA requests that the Commission treat certain information contained in this response as confidential for the previously identified reasons.

CURRENT INDUSTRY ACTIVITY (SIM-swap):

39. Each individual carrier has adopted their own measure to protect against unauthorized SIM-swap.

CURRENT INDUSTRY ACTIVITY (Fraudulent Ports):

40. Discussions by the WNP Council to identify an industry-wide solution began in May 2019. Over the course of these discussions, the WNP Council has focused on identifying a solution that will mitigate harm to consumers and can be implemented on an industry-wide basis. Numerous technical and business process issues were identified as requiring resolution to ensure the viability of the proposed solution across the disparate systems of each WSP.

41. In the interim, # # Discussions for additional measures continued.

42. # #

43. # :

- #

44. WSPs also took several confidential steps to augment their own internal processes.

45. In October 2019, the WNP Council held a two-day in-person meeting to review several different proposals to address the fraudulent ports issue and agreed in principal to an industry solution. Work was then undertaken by each WSP to review the solution internally and identify specific timelines for its implementation given the required changes to various internal systems and processes.

OVERVIEW OF NEW PROCESS:

47. The new WNP process will introduce additional measures that will enhance the verification process without unreasonably impeding the porting process. The WNP Council regards the technical details of the new process as being confidential as public disclosure of these details may enable fraudsters to better understand and circumvent these measures intended to protect Canadian consumers from fraud, exposing consumers to further harm.

46. #
#

#
47.
#

48. #
#

49. #
#

#
50.
#

51. #
#

52. #
#

53. # # # #

54. # # # #

55. # #

Question 7: An indication of the CWTA's plan to engage non-members in any described process improvements and to educate the public as appropriate

WSP TRADING PARTNER ENGAGEMENT:

56. WSPs participating in the WNP Council provide wireless service for most Canadian consumers. Implementation of the new system and process changes should therefore safeguard a significant portion of consumers.

57. To ensure that non-participating WSPs are aware of the work underway, WNP Council members will identify their Trading Partners[4], and CWTA will advise of the changes which will be made, as well as the timing of these changes.

WIRELINE TRADING PARTNER ENGAGEMENT:

58. The WNP Council does not anticipate an impact on wireline Trading Partners, however, it will likely be necessary to update the Canadian Local Ordering Guidelines (C-LOG) to reflect mapping requirements associated with the implementation of system changes.

59. Discussions related to C-LOG will occur within CRTC Interconnection Steering Committee (CISC) Business Process Working Group (BPWG) forums, using the currently defined BPWG process.

CONSUMER ENGAGEMENT:

60. Consumer awareness activities will be the responsibility of each WSP since many of the Account Holder / Authorized User validation processes being developed are specific to each carrier and, to a degree, identified customer preference.

[4] For the purposes of this RFI, a trading partner is any WSP that does not participate on the WNP Council but has a reciprocal porting arrangement with one or many WNP Council members.

61. CWTA will discuss with its members opportunities to inform stakeholders of new industry processes that may be relevant to work they undertake, and to inform consumers how they may more proactively safeguard their personal information.

CONCLUSION:

62. Our stakeholders have put considerable time, effort, and resources into identifying viable industry-wide solutions to address issues of customer security and privacy as they are identified.

63. As fraudsters' methods evolve, so do the efforts of the wireless industry. CWTA and the members of the WNP Council will continue to work collaboratively to protect Canadian consumers as issues become known.

Sincerely,

[*ORIGINAL SIGNED BY ERIC SMITH*]

Eric Smith
Senior Vice President

c.c.: CRTC Registered Wireless Carriers
Ursula Grant ugrant@cwta.ca
Bill Mason bill.mason@crtc.gc.ca

*** End of Document ***