The Fraudsters' Port of Entry: Putting an end to the 'SIM-swap Scam' in Canada

Briefing for the Standing Committee on Industry, Science, and Technology

Randall Baran-Chong
Co-Founder, Canadian SIM-swap Victims United
March 12, 2020

“WNP (*Wireless Number Portability*) is a **consumer-friendly** initiative that will provide **more choices** to consumers and a **more competitive** service marketplace…It is in-line with our government's goal of reshaping the telecommunications sector to benefit consumers…”

- Maxime Bernier, Minister of Industry, March 14, 2007[1]

While well-intended; this convenience opened a door to fraudsters through the **SIM-swap scam**

SIM*-swap Scam

aka. “unauthorized customer transfer”, “unauthorized porting”, etc.

The transfer of a person’s phone number from their SIM to another without the authorization of the account holder.

* – Subscriber Identity Module

Anatomy of a SIM swap scam*

1 "Gathering the Goods"

The Target

Gather personal and port-required info[2]:

- Phone # **&** one of:
- Account #,
- Device ID (e.g., IMEI),
- PIN

The Method

- Social engineering (the carrier)
- Phishing
- Open info (e.g., social media)
- Data leaks (e.g., Koodo breach[3])
- Inside employees

2 Executing the Port

Create a New Carrier Account

With no personal ID required, fraudster gets a prepaid phone

Fraudster Requests Port

With correct info, new carrier executes transfer from customer's carrier **within 2.5 hrs**[4]

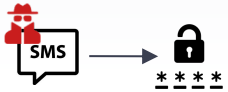
Customer Out-of-Service

SIM is disconnected from the network

3 Taking Ownership

Port Completed

All calls and texts are now routed to the fraudster



"Forget-It-and-Reset-It"

Identify common accounts using SMS-based 2-factor authentication[5] (2FA), and "reset passwords" to lock out customer

Customer identifies,

reports fraud

4 Plunder

"Systematic Havoc"

Fraudsters work at speed through accounts, including:

- E-mail
- Crypto accounts
- Online banking
- Credit card-linked apps
- Cloud storage
- Social media

Account Recovery

Customer contacts their original provider (hours to days to reclaim)

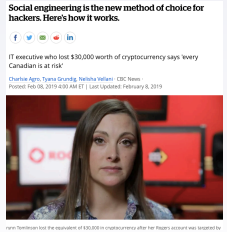
* – Illustrative to reflect a "common case" scenario from primary & secondary research

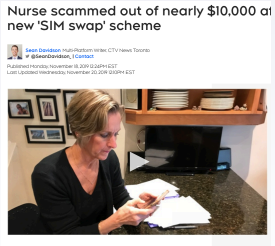
How the damage is done…

Direct theft:

Access bank accounts or crypto wallets

Make online purchases





Data theft:

Extortion/blackmail money

Monetize data/identity on the "Dark Web"

"Market prices"[6]:

Login creds: $20-120

Full ID: $3,000+

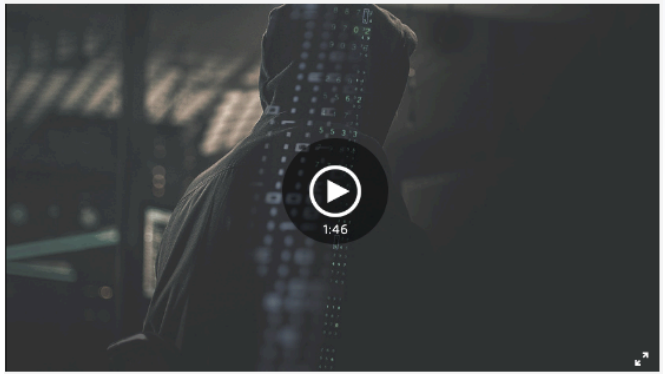
Account takeover or impersonation:

"OG" accounts

Note: Images link to media source

…and Canadians are “cashing in”

Un présumé pirate montréalais aurait volé des millions en cryptomonnaie



Un jeune crack en informatique de 18 ans, dont la résidence des parents a fait l’objet d’une perquisition à Montréal par la police de Toronto et la Sûreté du Québec en novembre dernier, est soupçonné de faire partie d’un cercle de pirates informatiques qui a dérobé des dizaines de millions de dollars en accédant aux téléphones cellulaires de détenteurs de cryptomonnaies.

In Nov. 2019, an 18 year-old Montreal resident was arrested for their participation in the **theft of $300,000 in Canada, and $50,000,000 in cryptocurrency from Americans**[7]

SIM-swaps are **‘low-tech’** – relying on human fallibility; many of those charged in the US and Canada are under the age of 25[8]

The reality is:

Our phone numbers are our **new form of identity**;

Security is as "**strong as the weakest link**" – whether it's a technical or human-factor;

Unauthorized porting, while not widespread, has a **devastating, lifetime impact**;

There's no perfect solution, but **education, cooperation, and a paradigm shift towards non-SMS 2FA can fight it**.

Ultimately, all Canadian wireless customers are at risk.

How it's being dealt with elsewhere

US: SIM-Swap Scams Taken as a Serious Threat

Bicameral Letter from Sen. Ron Wyden to FCC Chairman Pai (Jan. 2020)[9]

Endangers consumers: via financial frauds (est. $70M, 3,000 + cases), and privacy breaches

Endangers National Security: a "…cyber criminal or foreign government using a SIM swap to hack…"; may be used against "a local public safety official…to issue emergency alerts"

Actions: review of regulations and identify reforms

Global: Collaboration in Fraud Risk ID'ing

Data-sharing reforms across Africa[10]

MZ Initiated real-time information sharing in 2018: a "Y/N" API to identify whether the customer executed a port within a given time as a risk-based approach in identifying money transfers to flag

Actions: Similar approaches adopted in ZA, KE, NG

AU: Regulatory Reform to Reduce UP

ACMA codifies new measures[11,12]

Introduced a new pre-porting process: new carrier contacts via call or text before port (or in-person w/ Gov't. ID)

Fines of up to $250,000 for poor verification processes

Public education by the telcos of these measures

Actions: announced Feb 28, 2020; implement April 30, 2020

The Canadian 'hang-up' on porting fraud

CRTC/CWTA Communications on Unauthorized Porting

- Oct. 2019: WNP* Council forms "agreement in principle"; providers review own timelines[13]
- Jan. 15, 2020: CRTC letter[14] to CWTA on UP: status, prevalence, actions, etc.
- Feb. 14, 2020: CWTA, telco responses[15,16] -- **no public disclosure of #s or actions**

Actions-to-date by the Providers[18]

- **Practices vary** by provider
- Inconsistencies in protections offered **by customer service reps**
- **Frauds continue** with text notification of port, 'call if not your request' solution:
  - Skepticism of the text[19]
  - Executed too quickly to act[20]
  - Unable to reach hotline[21]

Public Engagement in UP Reduction

- Jan. 21, 2020: PIAC letter to request Notice of Consultation[21]
- Jan. 30, 2020: CWTA response – **"public consultation will not add any value..."** [22]
- **Victim stories are greatest "promoter"** of UP awareness
- Lack of awareness of more secure **alternatives** to SMS-based 2FA

Concern

"Security through obscurity" fallacy[17]

No indication of how CRTC is evaluating / measuring / enforcing

Inconsistent, ineffective practices within/between providers

Ignorance of issue and solutions by public (until it's too late) – and not just the vulnerable

* – The Wireless Network Portability (WNP) Council consists of Bell, Eastlink, Freedom Mobile, Rogers, SaskTel, Tbaytel, TELUS, and Videotron

The Canadian ‘call to action’

Ask: A consistent, “friction-minimal” solution

CRTC to codify a pre-porting authorization practice into the WNP regulations (akin to AU policy)

CRTC study with CWTA on feasibility of adopting additional protections (e.g., mandatory PIN)

Ask: Greater transparency/accountability

CRTC reporting on WNP Council plan (including employee training, stakeholder engagement)**, progress, UP prevalence, and implementation enforcement**

Ask: Investment in public education

Study/expedite adoption of non-SMS based 2FA in key agencies and industries

Public campaign on authentication-factor risks and secure alternatives

Thanks for your time.
Let's turn porting into a safer harbour.

Canadian SIM-swap Victims United | March 12, 2020

References

1. "Wireless Portability Now Available in Canada" https://www.canada.ca/en/news/archive/2007/03/wireless-number-portability-now-available-canada.html
2. "Canadian Wireless Telecommunications Association (CWTA) response to CRTC file: 8665-C12-202000280": https://crtc.gc.ca/public/otf/2020/c12_202000280/3806745.pdf
3. "Telus Says Koodo Suffered Data Breach Leaking Account and Phone Numbers": https://www.iphoneincanada.ca/carriers/telus/telus-koodo-data-breach/
4. "Telecom Decision CRTC 2005-72": https://crtc.gc.ca/eng/archive/2005/dt2005-72.htm
5. "Two Factor Auth List": https://twofactorauth.org/#social
6. "IMF: The Truth About the Dark Web", Sept. 2019: https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm#targetText=A%20recent%20report%20by%20a,than%20%241%20billion%20in%202019.
7. "Un présumé pirate montréalais aurait volé des millions en cryptomonnaie": https://www.lapresse.ca/actualites/justice-et-faits-divers/202001/12/01-5256560-un-presume-pirate-montrealais-aurait-vole-des-millions-en-cryptomonnaie.php
8. "The Rise of SIM Swapping": https://www.nasdaq.com/articles/the-rise-of-sim-swapping%3A-how-and-why-bitcoiners-need-to-protect-themselves-2020-02-04
9. "010920 SIM Swap Scam Letter to FTC", January 9, 2020: https://www.wyden.senate.gov/imo/media/doc/010920%20SIM%20Swap%20Scam%20Letter%20to%20FTC.pdf
10. "The SIM Swap Fix That the US Isn't Using ": https://www.wired.com/story/sim-swap-fix-carriers-banks/
11. "Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020": https://www.legislation.gov.au/Details/F2020L00179
12. "ACMA Announces New Measures to Fight Mobile Number Fraud": https://www.acma.gov.au/articles/2020-02/acma-announces-new-measures-fight-mobile-number-fraud
13. "CWTA response to CRTC file: 8665-C12-202000280": https://crtc.gc.ca/public/otf/2020/c12_202000280/3806745.pdf
14. "Telecom Commission Letter addressed to Mr. Eric Smith (Canadian Wireless Telecommunications Association)": https://crtc.gc.ca/eng/archive/2020/lt200115.htm
15. "CWTA response to CRTC file: 8665-C12-202000280": https://crtc.gc.ca/public/otf/2020/c12_202000280/3806745.pdf
16. "Fraudulent Wireless Customer Transfers – 2020 – 01 – 15": https://crtc.gc.ca/otf/eng/2020/8665/c12_202000280.htm
17. "What is Security Through Obscurity?": https://securitytrails.com/blog/security-through-obscurity
18. "CRTC Should Open Public Consultations to Update Port Protection, Industry Experts": https://ca.finance.yahoo.com/news/crtc-should-open-public-consultations-to-update-existing-number-port-protection-industry-experts-143838064.html
19. "New scam uses your phone number to steal your online identity": https://winnipeg.ctvnews.ca/new-scam-uses-your-phone-number-to-steal-your-online-identity-1.4815791
20. "Vancouver man says scammers stole his phone number to access his online accounts": https://vancouversun.com/news/local-news/vancouver-man-says-scammers-stole-his-phone-number-to-access-his-online-accounts
21. "London woman recounts cellphone scam that led to theft of passwords, number": https://lfpress.com/news/local-news/london-woman-victim-of-cellphone-porting-scam
22. Public Interest Advocacy Centre (PIAC) Letter to CRTC Requesting Commission to Issue a Notice of Consultation: https://crtc.gc.ca/public/otf/2020/c12_202000280/3791193.pdf
23. CWTA response to PIAC January 21, 2020 Letter: https://crtc.gc.ca/public/otf/2020/c12_202000280/3797644.pdf