

## Mint Mobile hit by a data breach after numbers ported, data accessed

By Lawrence Abrams

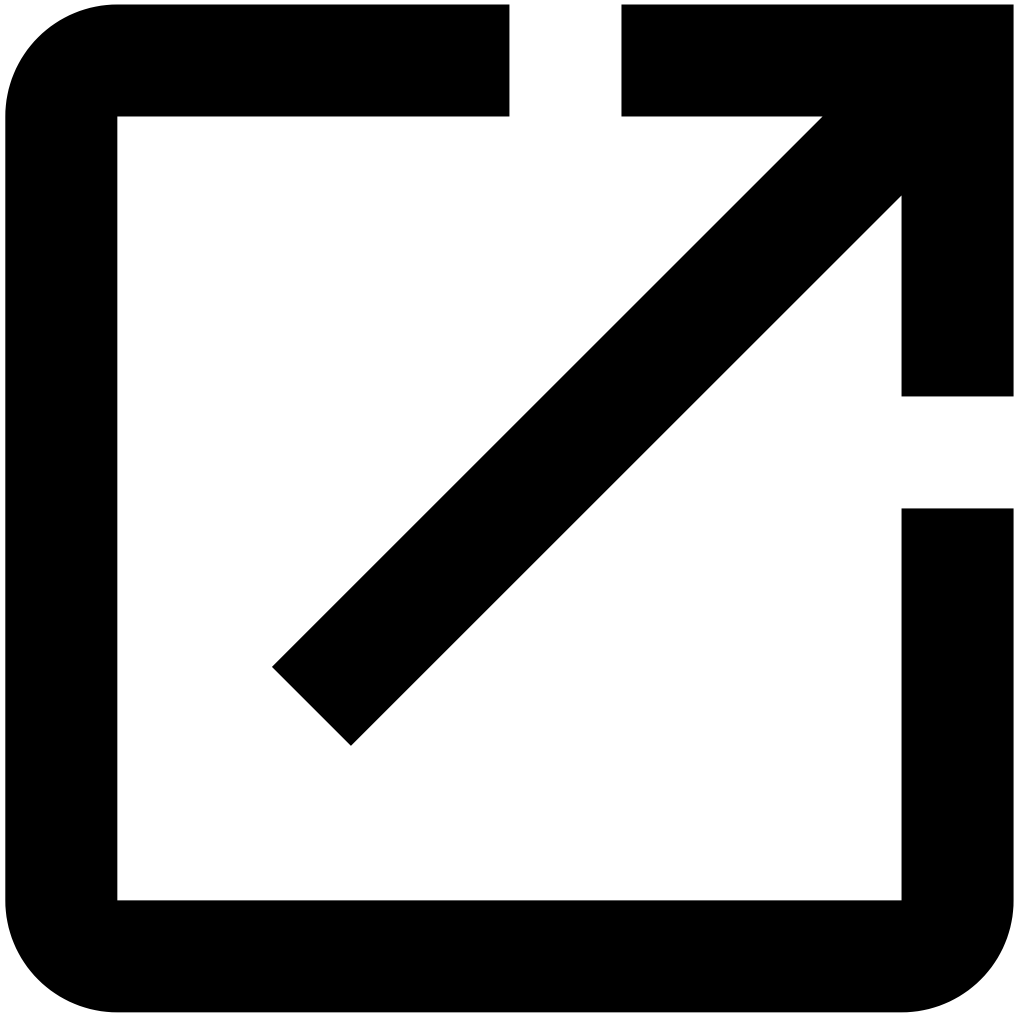
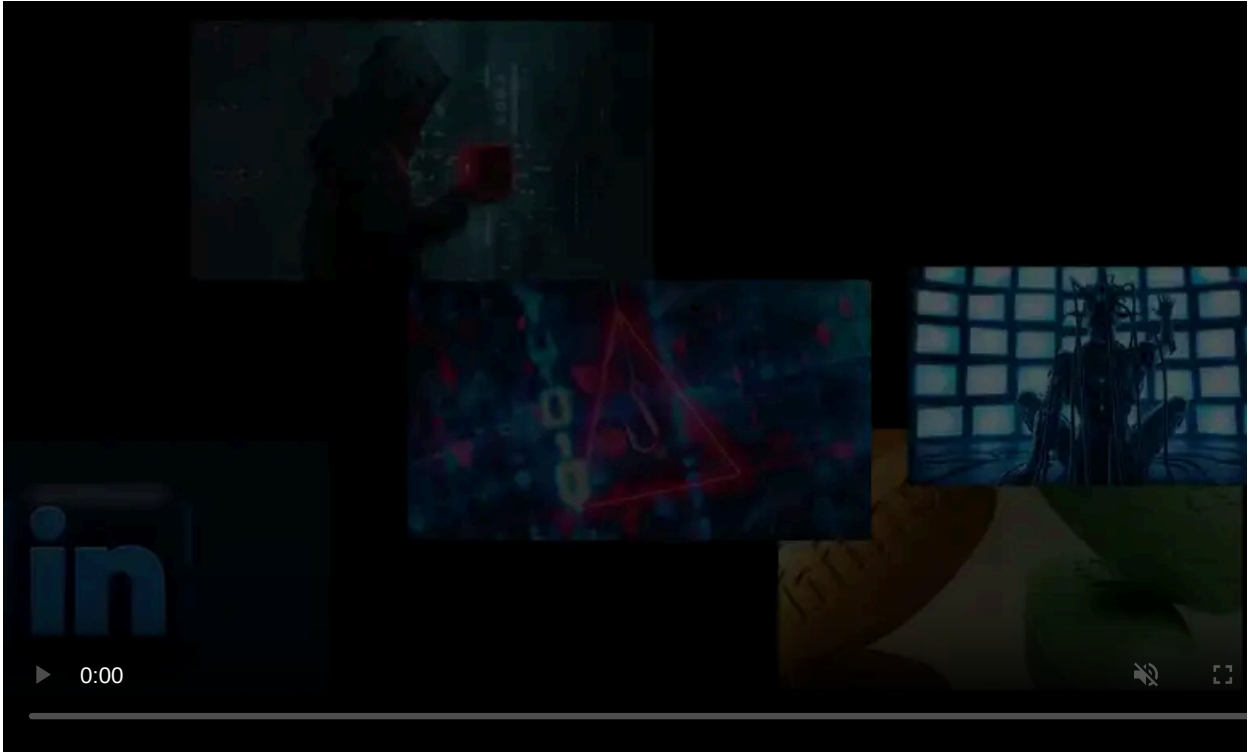
Published: 2021-07-10 · Archived: 2026-04-05 18:29:43 UTC



Mint Mobile has disclosed a data breach after an unauthorized person gained access to subscribers' account information and ported phone numbers to another carrier.

According to the data breach notification email sent to affected subscribers this weekend, between June 8th and June 10th, a threat actor ported the phone numbers for a "small" number of Mint Mobile subscribers to another carrier without authorization.

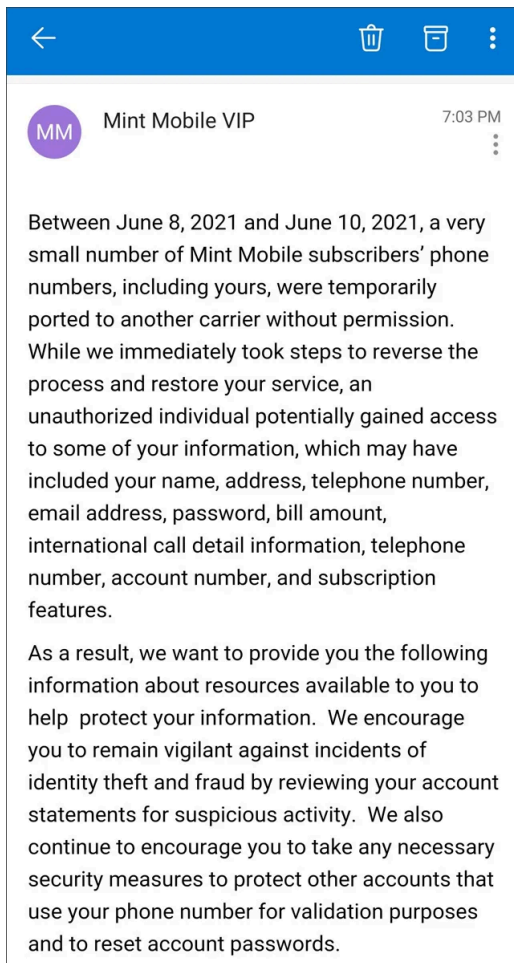
In addition to the ported number, Mint Mobile disclosed that an unauthorized person also potentially accessed subscribers' personal information, including call history, names, addresses, emails, and passwords.



Visit Advertiser website [GO TO PAGE](#)

"Between June 8, 2021 and June 10, 2021, a very small number of Mint Mobile subscribers' phone numbers, including yours, were temporarily ported to another carrier without permission," Mint Mobile disclosed.

"While we immediately took steps to reverse the process and restore your service, an unauthorized individual potentially gained access to some of your information, which may have included your name, address, telephone number, email address, password, bill amount, international call detail information, telephone number, account number, and subscription features."



**Mint Mobile data breach notification**

Source: [Reddit](#)

While Mint Mobile has not said how the threat actor gained access to subscribers' information, based on the accessed data, it is likely that hackers hacked user accounts or compromised a Mint Mobile application used to manage customers.

As the threat actors may have gained access to your Mint Mobile password, it is strongly advised that you change your password on your account.

Furthermore, threat actors could have used the ported number additional attacks, such as phishing, or to gain access to 2-factor authentication codes sent via text message.

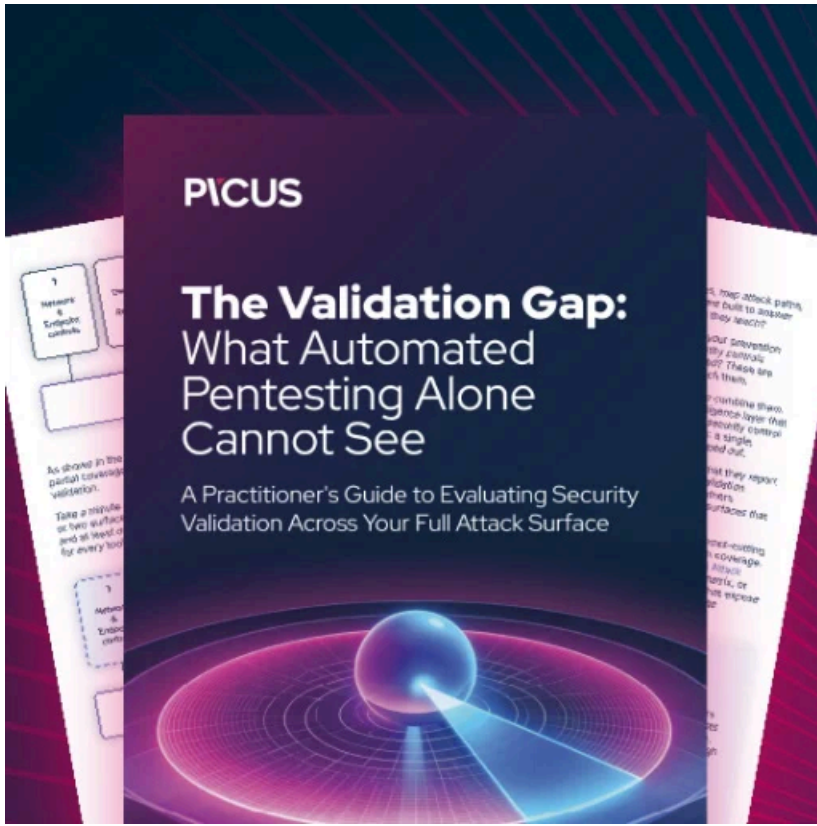
Due to this, Mint Mobile is warning affected users to "protect other accounts that use your phone number for validation purposes and to reset account passwords."

USCellular disclosed a similar attack in January after threat actors scammed employees into download software that provided remote access to the company's devices.

Using this remote access, the hackers used customer relationship management (CRM) software to access subscriber's personal information and port their numbers.

BleepingComputer has reached out to Mint Mobile for more information but has not heard back as of yet.

Thx to [@CatgirlDev](#) for the tip!



### **[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)**

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/mint-mobile-hit-by-a-data-breach-after-numbers-ported-data-accessed/>