

Australian Man Sentenced for Scam Related to Optus Hack

Australian authorities this week announced the sentencing of a Sydney man for attempting to blackmail Optus customers using leaked data stolen during a September 2022 data breach at the wireless carrier.

The Optus hack resulted in the theft of personal information belonging to 9.8 million customers, including names, birth dates, physical and email addresses, and phone numbers. For 2.1 million customers, numbers associated with identification documents were also compromised.

The incident was disclosed on September 22, with the attackers leaking the personal information of roughly 10,000 individuals a few days later.

The attackers demanded a \$1 million ransom in cryptocurrency, threatening to release more of the stolen information each day until a payment was made.

On October 6, the Australian Federal Police announced the arrest of a Sydney man who attempted to use the leaked data to extort money from individuals impacted by the data breach.

The man, now 20, sent text messages to more than 90 Optus customers, demanding that they transfer \$2,000 AUD (roughly \$1,300 USD) to a bank account in the name of the scammer.

The youngster pleaded guilty on November 8 to two “counts of using a telecommunications network with intent to commit a serious offense [...], where the serious offense is blackmail”, the Australian authorities say.

The individual was sentenced to 18-month community correction order and 100 hours of community service.

Related: Email Hack Hits 15,000 Business Customers of Australian Telecoms Firm TPG

Related: Hackers Leak Australian Health Records on Dark Web

Related: Medibank Confirms Data Breach Impacts 9.7 Million Customers

Australian Man Sentenced for Scam Related to Optus Hack