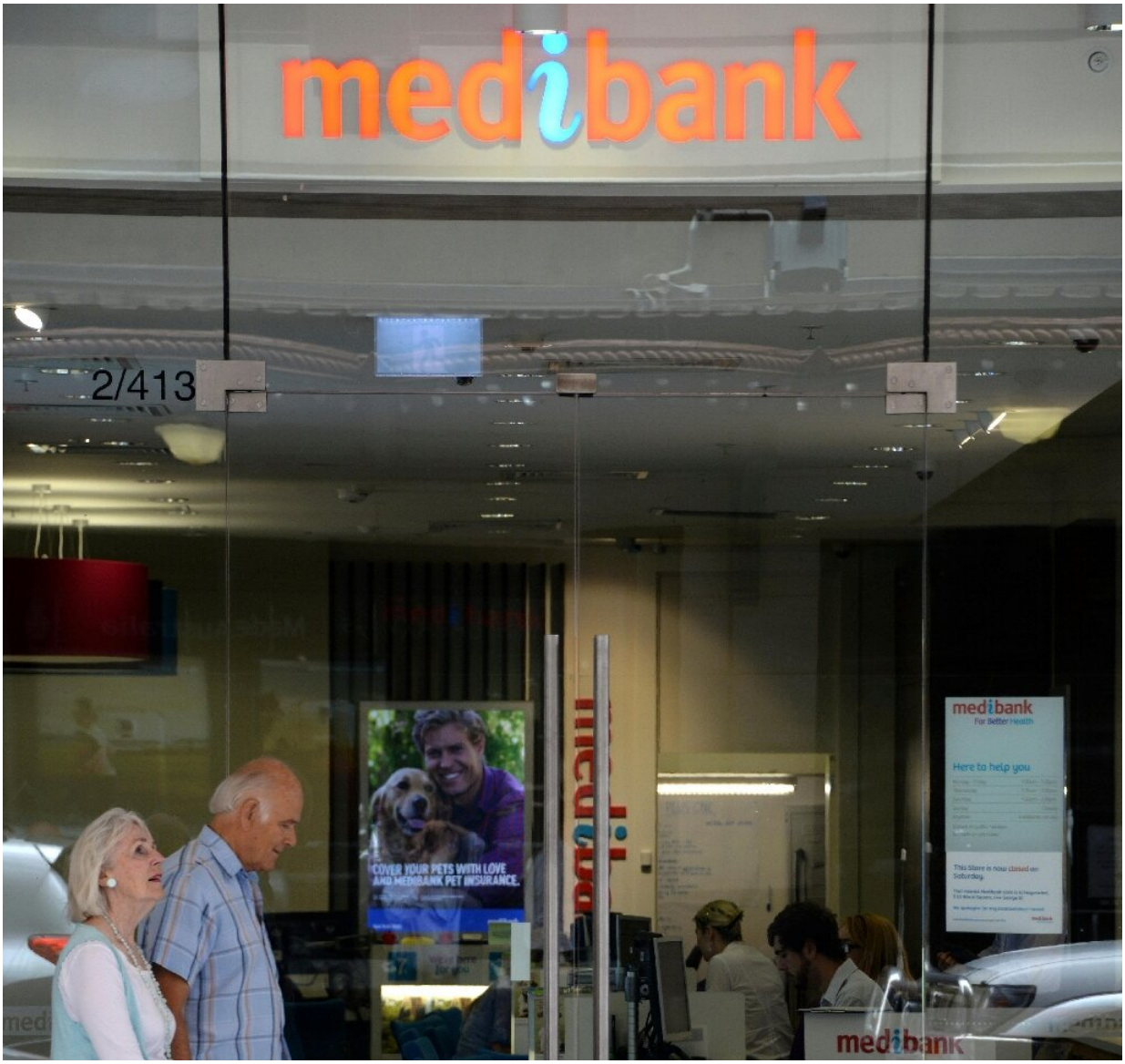
Australian insurer warns of 'distressing' hack threat

November 8 2022



Medibank Private, one of Australia's largest insurers, has told customers to be

"vigilant" after a purported hacker threatened to release data within 24 hours from a hack affecting 10 million people.

A major Australian health insurer warned Tuesday of a "distressing" threat by a purported hacker to release client data within 24 hours, following a hack affecting 10 million people.

Medibank Private, one of Australia's largest insurers, told customers to be "vigilant" after the reported threat, issued a day after it had ruled out paying any ransom demand.

The company revealed Monday that a hack originally thought to have breached the data of 3.9 million people had in fact given access to the names, birth dates, addresses, phone numbers and emails of about 9.7 million former and existing clients.

Those numbers included 1.8 million international customers.

On Tuesday, an anonymous poster on a hacking blog—widely cited by Australian media—said that data from the Medibank hack "will be publish in 24 hours".

It was not possible to confirm whether the poster was connected to the hack or had access to people's stolen information.

"We knew the publication of data online by the criminal could be a possibility, but the criminal's threat is still a distressing development for our customers," Medibank chief executive David Koczkar said, calling for clients to be "vigilant".

"We unreservedly apologise to our customers," he added.

The hacker could also attempt to contact customers directly, the company warned.

'Betrayal'

Medibank had said in Monday's announcement that it believed "all of the customer data accessed could have been taken by the criminal".

The data breach included some people's health claims along with codes exposing their diagnoses and medical procedures, as well as the passport numbers and the visa details of international students.

Medibank said it was working with the Australian government and with the police, who were trying to prevent the sharing and sale of the stolen data.

Cybercrime experts had advised that paying a ransom had only a "limited chance" of ensuring the return of the stolen data, the company said, explaining its decision to reject any ransom demand.

Two law firms said Tuesday they had joined forces to investigate a possible class action lawsuit against Medibank.

"We believe the data breach is a betrayal of Medibank Private's customers and a breach of the Privacy Act," said a joint statement by Bannister Law and Centennial Lawyers.

"Medibank has a duty to keep this kind of information confidential."

The Medibank hack followed an attack on telecom company Optus in September that exposed the personal information of some nine million Australians.

As data theft becomes more common, it may raise questions over the need for Australian businesses to gather customers' sensitive personal information, said Michael Duffy, associate professor of corporate law at Monash University.

Some of those data retention policies were dictated by government regulation, he added.

"Nevertheless, businesses requesting and keeping personal details that aren't completely essential could become more legally problematic for them, if they are hacked."