Named and shamed: For the first time, Australia enforces cyber sanctions against Medibank hacker

DENTONS

January 29, 2024

Key Points

- The Australian Government has named Russian citizen Aleksandr Ermakov as the cybercriminal behind the 2022 Medibank data breach, and he becomes the first person to be designated under Australia's autonomous cyber sanctions framework.
- Mr Ermakov will be subject to asset restrictions and a travel ban. Any person who assists Mr Ermakov in breach of the sanctions may face up to 10 years' imprisonment and heavy fines.
- The decision to name the hacker demonstrates Australia's "name and shame" approach to cyber criminals, hoping to significantly disrupt their business and syndicates internationally.

Background

Fifteen months after the Medibank cyber incident, the Australian Government has named Aleksandr Ermakov, a 34-year-old Russian citizen, as the cybercriminal responsible for the data breach.

In a joint media release on 23 January 2024, the Australian Minister for Foreign Affairs Penny Wong, alongside Minister for Home Affairs Clare O'Neil and Deputy Prime Minister and Minister for Defence Richard Marles, announced they would use the cyber incidents sanctions regime (**Sanctions Regime**) for the first time in response to this "egregious violation".

The Medibank data breach involved the harvesting of 9.7 million records from Australia's largest health insurer in October 2022, including names, addresses, birth dates, Medicare numbers and sensitive health information of then current and former Medibank customers. Controversially, the hackers ultimately posted this data on the dark web.

With assistance from agencies in the UK and the USA, including the FBI, the Australian Signals Directorate (**ASD**) and Australian Federal Police (**AFP**) have conducted a forensic investigation over the last 18 months to definitively link Mr Ermakov to the data breach.

The use of the Sanctions Regime against the Medibank hacker marks the first time the cyber sanctions laws have been enforced in this manner since their introduction in December 2021. The sanctions are reserved for the most egregious situations of international concern and designed to:

- have broad application;
- penalise persons or entities either attempting, causing, assisting with causing, or who are complicit in significant

cyber incidents which result or seek to result in significant harm; and

- capture such conduct occurring anywhere in the world.

However, the Minister for Foreign Affairs may grant a permit authorising certain activities that would otherwise violate the Sanctions Regime if proven that such activities are in Australia's national interest.

Impact

As a result of the sanctions, Mr Ermakov is subject to restrictions on assets and a travel ban. Consequently, he will be unable to enter or transit through Australia, and any individuals who try to provide assets to Mr Ermakov or use or deal with his assets, including through cryptocurrency wallets or ransomware payments, will be met with up to 10 years' imprisonment and significant financial penalties.

The naming and identifying of Mr Ermakov symbolises Australia's approach to name and shame cyber criminals, with the aim to significantly disrupt their business and syndicates. The AFP and ASD have now charged Mr Ermakov in absentia and put a warrant out for his arrest, with the hope that he will be placed on watch lists internationally.

The international effectiveness of Australia's action has been significantly bolstered by the UK and USA governments also designating Mr Ermakov under their respective sanctions regimes.

Next steps

With the increasing prevalence of major cyber attacks on enterprise infrastructure and better technological solutions to identify the hackers, especially with international cooperation, we expect to see more examples of the Sanctions Regime being activated in the future.

Please contact your usual Dentons privacy and cyber expert if you require assistance on these matters.

Your Key Contacts

Michael Park
Partner, Melbourne
D +61 3 9194 8313
michael.park@dentons.com

Robyn Chatwood
Partner, Melbourne
D +61 3 9194 8330
robyn.chatwood@dentons.com

Matthew Hennessy
Partner, Melbourne
D +61 3 9194 8389
matthew.hennessy@dentons.com

Ben Allen
Partner, Sydney
D +61 2 9035 7257
ben.allen@dentons.com