Vanguard Investment Stewardship Voting Insights

Cyber risk at Medibank

February 2024

Company: Medibank Private Limited (Medibank)

Meeting date: November 22, 2023

Proposal: Item 2—Elect Mike Wilkins as Director; Item 3—Elect Tracey Batten as Director

How the funds voted

At the annual shareholder meeting of Medibank, an Australian-listed health company, the Vanguard-advised funds supported the re-election of both directors on the ballot, as we assessed that the board took a sensible, robust approach to risk governance and risk oversight following a cyberattack at the company.[1]

Vanguard's principles and policies

Good governance starts with a company's board of directors. Our primary focus when evaluating a company's governance practices is ensuring that the individuals who serve as board members represent the interests of all shareholders and can demonstrate effective, independent oversight of the company's management team, strategy, and risks to long-term shareholder returns.

Vanguard's Investment Stewardship team seeks to understand how boards oversee company strategy and material risks to long-term financial performance. We look for boards to take a thorough, integrated, and thoughtful approach to identifying, quantifying, and mitigating risks that have the potential to affect shareholder returns over the long term. We also look for boards to communicate their approach to risk oversight transparently through engagement and written disclosures. If we identify material governance failures where a board has failed to effectively identify, monitor, and ensure management of material risks, the funds may vote against the relevant board committee chair and/or the board chair to reflect concerns regarding risk oversight.

Analysis and voting rationale

In October 2022, Medibank was subject to a cybercrime event whereby, according to public reports, personal data related to approximately 9.7 million current and former customers and employees was accessed and stolen. The company has disclosed that stolen login credentials from a third-party IT service provider were used to access Medibank's network

1 Vanguard's Investment Stewardship program is responsible for proxy voting and engagement on behalf of the quantitative and index equity portfolios advised by Vanguard (together, "Vanguard-advised funds"). Vanguard's externally managed portfolios are managed by unaffiliated third-party investment advisors, and proxy voting and engagement for those portfolios are conducted by their respective advisors. As such, throughout this document, "we" and "the funds" are used to refer to Vanguard's Investment Stewardship program and Vanguard-advised funds, respectively.

through a misconfigured firewall. In November 2022, it was disclosed that the stolen data had been released onto the dark web following the company's decision not to provide ransom payments in exchange for the data. Following the data breach, the company was the subject of multiple class-action lawsuits, a formal investigation by the Office of the Australian Information Commissioner (OAIC), and an additional capital adequacy requirement of A$250 million by the Australian Prudential Regulation Authority (APRA). The incident cost the company A$46 million, with the costs estimated to exceed A$76 million by the end of 2024.

At the 2023 annual meeting, the board's chair and a non-executive director who was also a member of the board's Risk Management Committee were on the ballot for re-election. The funds voted to re-elect both directors because, through our engagements and research of the situation, we determined that the board had a robust response to the incident. That response included an incident review conducted by a third party, adjustments to executive remuneration in light of the event, ongoing cooperation with regulators, and effective communication with and disclosure to shareholders.

Following the data breach, Deloitte was engaged to conduct an external incident review of the event. Recommendations were made by Deloitte to enhance the company's IT processes and systems, which the company continues to implement, along with other enhancements previously planned by it.

Also in response to the incident, the Medibank board exercised downward discretion for key management personnel such that no short-term awards were granted in FY 2023. This was done to respect the expectations of Medibank customers, shareholders, and the community.

Regarding the company's ongoing cooperation with regulators, Medibank has continued to adhere to APRA's capital adequacy requirement, seeking to reach agreed-upon remediation milestones. Medibank also has continued to cooperate with the OAIC and its ongoing investigation, and Medibank has acknowledged that the investigation may result in future fines, penalties, or other regulatory enforcement action. As of December 2023, Medibank's share price had largely recovered since the cyberattack, with the company achieving a positive one-year total shareholder return. It also achieved net customer growth in 2023, surpassing four million customers for the first time in its history.

Following the cyber event, the Medibank board proactively contacted investors, including Vanguard's Investment Stewardship team. We engaged twice with the company's directors—once not long after the event occurred and again about a year after it. During each engagement, the company's directors were forthcoming about the event and were able to speak in detail about the board's oversight of cybersecurity-related risks. They confirmed that following the incident, the company continues to mature its risk management culture and practices through its broader IT security uplift program. Since the cyberattack, the company has also published detailed disclosures about the incident in its Sustainability Report, Annual Report, and Half-Year Results; those disclosures have given shareholders visibility into the impact of the breach on the company, remediation efforts that are underway, and the actions that have since been taken to enhance Medibank's internal systems and to provide additional support to customers.

In light of these factors, we ultimately determined that the board's response to the cyberattack was sensible and robust, and we supported the re-election of both directors on the ballot.

Vanguard publishes Investment Stewardship Policy and Voting Insights to promote good corporate governance practices and to provide public companies and investors with our perspectives on important governance topics and key votes. This is part of our effort to provide useful disclosure of Vanguard's investment stewardship voting and engagement activities. We aim to provide clarity on Vanguard's stance on governance matters beyond what a policy document or a single vote can provide. Insights should be viewed in conjunction with the most recent region- and country-specific voting policies.

The funds for which Vanguard acts as investment advisor (Vanguard-advised funds) retain the authority to vote proxies that the funds receive. To facilitate the funds' proxy voting, the boards of the Vanguard-advised funds have adopted Proxy Voting Procedures and Policies that reflect the fund boards' instructions governing proxy voting. The boards of the funds that are advised by managers not affiliated with Vanguard (external managers) have delegated the authority to vote proxies related to the funds' portfolio securities to their respective investment advisor(s). Each external manager votes such proxies in accordance with its own proxy voting policies and procedures, which are reviewed and approved by the fund board annually.

Vanguard®

3365279 022024