

## Railpen question – cybersecurity

I am asking this question on behalf of Railpen, the investment arm of the UK railways pension schemes. We are part of a broader coalition of investors with over \$475 billion in assets under management, engaging with companies to understand their approach to cybersecurity.

As investors, we recognise the substantial threats that cyber attacks and breaches can pose to our portfolio companies. These can result in fines, loss of revenue and reputational harm that in turn can affect the financial outcomes we provide to our beneficiaries.

In light of the critical role companies like AbbVie play in the healthcare ecosystem, your extensive and growing digital footprint, and the level of sensitive data you hold, we welcome your commitment to invest in the protection of your data and information technology.

We recognise that the very nature of cybersecurity means that information can be deemed too sensitive for public disclosure. However, given the materiality of the issue, investors need sufficient understanding of a company's approach to cybersecurity in terms of its governance, risk and controls management, and its approach to building a culture of cyber awareness amongst employees, suppliers and customers. As previously requested, will the Chair of the Board, or relevant Board Director, agree to meet with Railpen and other representatives of our cybersecurity investor coalition to discuss these important issues further?