ASX release

16 November 2022

Chair and CEO AGM presentations and FY23 Outlook Update

In accordance with the ASX Listing Rules, Medibank releases to the market the addresses to security holders to be delivered by the Chair, Mike Wilkins AO and the Chief Executive Officer, David Koczkar, at Medibank's 2022 Annual General Meeting to be held at 10.30am today, along with an update to its FY23 outlook.

This document has been authorised for release by Mei Ramsay, Company Secretary.

For further information please contact:

For media

Emily Ritchie
Senior Executive, External Affairs
M: +61 429 642 418
Email: Emily.Ritchie@medibank.com.au

For investors/analysts

Colette Campbell
Senior Executive, Investor Relations
T: +61 475 975 770
Email: investor.relations@medibank.com.au

CHAIR

Good morning everyone. My name is Mike Wilkins and on behalf of the Board I'd like to welcome you to the 2022 Medibank AGM.

As we begin, I would like to invite Wurundjeri Elder, Uncle Dave Wandin, to open today's proceedings with a Welcome to Country. Thank you for being with us, Uncle Dave.

We are committed to helping advance reconciliation and believe it is important to recognise Australia's Traditional Owners and their continuing connection to Country. I respectfully acknowledge the Wurundjeri Woi Wurrung peoples of the Kulin nation, on whose lands we meet this morning and pay my respects to Elders past, present and emerging. I'd also like to extend that respect to all Aboriginal and Torres Strait Islander peoples joining us today.

Today's meeting is our first to be held in a hybrid format, so I'd like to thank all shareholders for joining us today, both those joining us virtually through our livestream and those here in the auditorium.

It's great to be able to meet with our shareholders in person for the first time since COVID began, albeit in undoubtedly challenging circumstances for Medibank and our customers.

I now formally declare the meeting open.

Joining me on stage today is the Medibank Board of Directors.

On your far left is Dr Tracey Batten who is Chair of the Board's People and Remuneration Committee, followed by Peter Everingham who is standing for election today. Next is Linda Nicholls who is Chair of the Investment and Capital Committee, and who is standing for re-election today, followed by our Chief Executive Officer David Koczkar.

On your far right is Anna Bligh, followed by Gerard Dalbosco who is Chair of the Audit Committee. Next we have Kathryn Fagg who is standing for election today, followed by David Fagan who is Chair of the Risk Management Committee, and is also standing for re-election. Finally, to your immediate right of me, is our Company Secretary Mei Ramsay.

I would like to begin today's meeting by addressing the cyberattack that we and our customers have been facing for a little over a month now.

This cybercrime event is unprecedented. It has caused distress and concern for many of our customers, our people and for you, our shareholders – many of whom I know are also customers.

I unreservedly apologise to every person for the significant impact of this crime. It is a despicable act by the criminal seeking to extort payment based on the privacy concerns of our customers and must be condemned in the strongest possible terms.

Throughout our almost 50-year history, our focus on customers and improving the health and wellbeing of all Australians, has been unwavering. It's the reason we were founded, and it's the reason we exist today.

There is no doubt that this crime is having an enormous impact on our customers and our community. This is a shocking crime – the size and scale of which we have never seen before.

But for each one of our customers impacted, we recognise that the impact is personal and the support that is required for each individual is different. Our utmost priority has been, and continues to be, supporting our customers.

Safeguarding our customers' data is a responsibility we take very seriously and we will continue to support all people who have been impacted by this crime. This is why we have put in place a dedicated Cyber Response Support Program for our customers, and David will speak more to this shortly.

From the very beginning, Medibank has committed to being transparent as events unfold and more is understood.

The ever-increasing risk of cybercrime is being faced by all organisations around the world – large and small. I want to reassure you that the Board has and will continue to invest in mitigating these risks.

Over the past few weeks, I've spoken with many of our major shareholders and advisors and I've been encouraged by the support they have shown us for how we are managing this event and the actions we are taking.

On behalf of the Board and all Medibank people, we thank all our stakeholders for their continued support during this time.

I would particularly like to thank the Australian Government, including the Australian Cyber Security Centre and the Australian Federal Police. We continue to work closely with them as the investigation and response to this crime progresses.

From the outset, Medibank has been committed to doing the right thing by our customers, our people and the community in relation to this cybercrime.

This includes our decision not to pay any ransom demand for this data theft.

Based on extensive advice from cybercrime experts, we formed the view that there was a limited chance paying a ransom would ensure the return of our customers' data and prevent it from being published.

In fact, the advice we have had is that to pay a ransom could have had the opposite effect and encouraged the criminal to directly extort our customers, and put more people in harm's way by making Australia a bigger target.

It is for these reasons we could not pay.

This decision is consistent with the position of the Australian Government.

In addition to our ongoing investigations and engagement with the Federal Police and Australian Cyber Security Centre, we have commissioned an external review, to be undertaken by Deloitte. This review will ensure that we learn from this cyberattack and continue to strengthen our ability to safeguard our customers.

We will share the key outcomes of the review, where appropriate, having regard to the interests of our customers and stakeholders and the ongoing nature of the Australian Federal Police investigation. We are also committed to sharing, where it is safe to do so, what we have learnt from our experience, so that Australian businesses and the broader community can be better placed to navigate any similar challenges in future.

The cybercrime event has understandably overshadowed many of our key achievements and our performance in FY22.

It was a challenging year for many Australians, with rising costs of living, flooding across much of eastern Australia and the ongoing impacts of COVID. Amid these challenges, our customers looked to us as they prioritised their health and wellbeing.

Notwithstanding the cybercrime attack we have continued to operate and to be there for our customers in order to help them with their health needs.

In FY22 we increased both Health Insurance operating profit and Medibank Health segment profit, however volatility in financial markets led to a $24.8 million loss in net investment income. As a result, our net profit after tax of $393.9 million was down 10.7% on the previous year.

We said at the release of the FY22 financial results that our capital position remained strong and the Board determined shareholders would receive a final fully franked ordinary dividend of 7.3 cents per share – an increase of 5.5 percent over the prior year – and this brought the total full year dividend to 13.4 cents per share fully franked.

Finally, while we had initially forecast FY23 policyholder growth of around 2.7%, we have since announced that the uncertain impact of the cybercrime has resulted in our withdrawal of this outlook statement. We will provide a further update at our February half-year results.

In closing, I'd like to take this opportunity to reflect on the important role that Medibank plays in our community.

This is an extremely challenging time, and we will continue to be measured on how we respond, and how we support our customers.

Our CEO David Koczkar and executive team have shown their ongoing focus on our customers, and they have not deviated from this during this time of adversity.

I am grateful to the whole Medibank team for their work, and the ongoing support they show our customers, and each other, every day.

Our 2030 vision is to deliver the best health and wellbeing for Australia. By always acting in line with our values, we remain well equipped to achieve it.

Finally, we thank you – our shareholders - for your ongoing support of the work we are doing to deliver Better Health for Better Lives for our customers and our community.

Throughout our history, we have responded to every challenge that has been laid before us.

I am confident that we will emerge from this cybercrime an even stronger organisation as we continue working to make a difference to the health and wellbeing of our customers, our people and our community.

I would like to take this opportunity to thank our people for the work that they have done to respond to this crisis and support our customers. Your focus on our customers is unwavering and the Board and I thank you for your commitment.

I'll now ask David to talk through the event in more detail, as well as speaking to our future direction and outlook.

CHIEF EXECUTIVE OFFICER

Thanks Mike, and good morning to everyone joining us in the room here today and on the webcast.

I begin by acknowledging the Traditional Owners and Custodians of country throughout Australia and their connections to land, sea and community. I join you today from Naarm, the home of the Wurundjeri Woi-Wurrung peoples. I pay my respects to their Elders past, present and emerging and I extend my respect to all Elders on the lands on which we work and live.

This morning I will start by addressing the cybercrime event we and our customers have faced over the past month. I will then recap our FY23 outlook and our focus for the year ahead.

Before I talk through the cybercrime in more detail, I want to again apologise unreservedly to our customers who have been the victims of this terrible crime.

What has happened is deeply distressing. The weaponising of the private data of many Australians – our customers – is malicious.

We are steadfast in our resolve to NOT reward this criminal behaviour, nor to strengthen a business model that is based on extortion.

This is a watershed moment for our community – a harsh reminder of the new frontier in cybercrime that we all face.

I am devastated for our customers - and I assure you our absolute focus is to continue to support and protect our customers through this time. And like Mike, I too am a Medibank customer.

Since the very first day our systems detected this unauthorised activity, we have continued to work closely with the Australian Government, including the Australian Cyber Security Centre and the Australian Federal Police, who are investigating this cybercrime.

Last week the AFP announced that Operation Guardian, a joint initiative with state and territory police, would be extended to protect Medibank customers.

AFP investigators under Operation Guardian are scouring the internet and dark web to identify people who are accessing this personal information and trying to profit from it. The AFP is also working with international agencies to disrupt the infrastructure of the criminal.

I would like to take this opportunity to re-iterate our thanks to the Australian Government. We are grateful for the support we and our customers have received from the government and its agencies as this crime has unfolded.

Whilst nothing is certain, the criminal may continue to release files on the dark web.

We share the Prime Minister's and the AFP's call to all media and social media platforms to protect the community by not posting or publishing this information. While we understand the public interest, reporting details of this crime only feeds the criminal's need for notoriety.

There is no doubt that rejecting the ransom demand was the right thing to do.

While we unreservedly apologise for the impact of the release of the data, we cannot as a community, pay criminals who are likely to continue to extort us all – particularly when there is no guarantee that the criminal would ever delete the data. As I've said before, you cannot trust a criminal.

For our customers, we know that this doesn't make up for the fact that your data has been stolen. We take our responsibilities seriously and have an unwavering focus on supporting our customers who have been impacted.

From the very beginning, we have committed to sharing updates on this unfolding situation with transparency and timeliness to all our stakeholders.

We have been focused on both communicating potential impacts to our customers and providing them with guidance and support.

I can confirm that in the last five weeks, we have regularly written to or spoken with our current and former customers to update them on the unfolding cybercrime.

Last week we began communicating with customers whose personal information we believe was stolen to advise them of the specific data that relates to them. And we have continued to email new groups of customers each day. Our customers can also contact us to understand what data has been accessed – we've extended call centre hours and we've increased our customer support team by more than 300 people.

Importantly, today we will begin communicating with around 480,000 customers whose health data we believe has been stolen. We commenced this as soon as this data was verified by our team.

Providing personalised updates to our customers is an incredibly complex process – and it is important to get it right. This ongoing work continues and requires our people to analyse millions of records across numerous applications and match customer data from multiple sources.

And for our customers whose health data has been published on the dark web, we've prioritised those communications, advising them as quickly as we can that their health data has been published, within 48 hours of this data appearing.

Right through this cybercrime, we've also proactively contacted our customers who we know are uniquely vulnerable, to provide them with additional support and care.

And three weeks ago, Medibank established a Cyber Response Support Program. This has been set up to provide customers with mental health and wellbeing support, identity protection, security and financial hardship measures.

We will continue to work around the clock to provide customers with details of their data we believe has been stolen and provide advice on what customers should do and how we can support them.

Our focus on supporting our customers has been and will continue to be our absolute priority.

Since we became aware of the cyberattack, we have worked to strengthen the integrity of our systems. We have applied additional security measures across our network including specialised tools to assist with our investigation and enable additional ongoing real-time monitoring for any further suspicious activity. And I can confirm that no further suspicious activity inside our systems has been detected since 12 October 2022.

As Mike has announced, the external review to be conducted by Deloitte, in addition to our ongoing investigation, will help us further strengthen our ability to safeguard our customers.

I want to reassure you that we continue to be vigilant and will take the necessary steps to protect our operations and our customers' data.

Mike has already provided an overview of our FY22 financial results, however I wanted to take this opportunity to acknowledge the strength of our result in what was another tough year for our customers and the Australian community.

The rising cost of living has presented a challenge for many households and yet a record number of Australians continue to take out private health insurance, putting their health and wellbeing first.

Consumers no longer see health spending as discretionary and are actually spending more on their health than before the pandemic. Our research tells us more people are valuing what private health insurance has to offer – including greater choice and access, especially given the increased awareness of the sustained pressures in the public health system, which we know will take some time to address.

More than 14 million Australians now have private health cover and Medibank is proud to play our part in supporting and strengthening the health system. As we have done for almost 50 years, we will be there to support our customers with their needs in health.

In FY22, we continued to grow by focusing on delivering leading customer experiences, differentiating our insurance business and expanding in health. This included a strong increase in our customers' adoption of our new health offerings, notably our prevention programs and new care models.

As I have said before, we will remain disciplined in how we grow and run our business.

In late October we provided a trading update for the first quarter of FY23 and updated our FY23 outlook. Our outlook for FY23 has not changed since this update.

As confirmed by Mike, given the uncertain impact of the cyber event, we have withdrawn our FY23 outlook for resident policyholder growth and will provide a further update at the half year 2023 results in February.

As at 12 November 2022, net resident policyholder numbers were in line with those at the end of the first quarter, with a growth of approximately 14,500 policyholders since the end of June 2022.

For the first quarter of this financial year, we've also seen continued growth in our non-resident business with approximately 14% customer growth since the end of June 2022. This means we now have the same number of customers in our non-resident portfolio as we did pre-pandemic.

Our outlook for underlying net claims expense per resident policy unit is unchanged at 2.3% for the full year and PHI management expense productivity initiatives remain in line with the FY23 outlook, and our expectation for inflation remains unchanged.

Importantly our business remains strongly capitalised, and at 30 September 2022, our health insurance capital ratio was 13.4%, and unallocated capital was approximately $150 million. APRA has released the final private health insurance capital standards which are effective from 1 July 2023 and we continue to expect the implementation of these standards will not negatively impact our capital position.

Supported by our strong capital position, we remain focused on pursuing multiple avenues of growth for our business, including targeted organic and inorganic growth for Medibank Health and Health Insurance, and delivering synergies across our businesses.

Based on our current actions in response to the cybercrime event, we currently estimate $25 million to $35 million of pre-tax non-recurring costs will impact earnings in the first half of 2023.

These non-recurring costs do not include further potential customer and other remediation, regulatory or litigation related costs.

There is no doubt that the cyberattack has been deliberate, designed to extort money by targeting our customers, particularly some of the most vulnerable people in our community.

We know that cybercrime is an ever present and growing threat. As a society we must stand together, to defend against the increasing risks faced by everyone in our community. We will do everything we can to ensure that we all learn from this and share the insights we can to better protect all Australians.

We have an incredible and passionate team of people who are exceptional at listening to our customers, understanding their needs and providing products and services to support them. And I want to thank each and every one of them for the support they are showing our customers, and each other, every day.

All of us at Medibank face an incredible challenge at present as we work to protect our customers. I am confident our team can get through this challenge and return to our focus on realising our 2030 Vision, by creating access, choice and control for our customers.

Together, we will learn, share and grow from this event and I remain confident that by focusing on our customers, we will continue to prosper.

Thank you.

I will now hand back to Mike to conduct the formal business of the meeting.

FY23 outlook update

Unchanged since the trading update on 26 October 2022

medibank

	FY23 outlook as presented at the FY22 Results	Current FY23 outlook
Customer relief	We continue to assess claims activity and any permanent net claims savings due to COVID-19 will be given back to customers through additional support in the future	No change to our commitment Deferral of premium increases for Medibank and ahm customers to 16 January 2023
Net Policyholder growth	c. 2.7% assuming a modest decline in industry participation growth in FY23 relative to FY22	FY23 Net Policyholder growth outlook withdrawn **Net resident policyholder growth update** • 1QFY23: +14.6k • YTD (as at 12 November 2022): approximately +14.5k
Claims	Given risk equalisation volatility, we expect underlying net claims expense per policy unit growth in FY22 of 2.3% to be the best indicator of growth in FY23 among resident policyholders	No change
Management expense in PHI	Productivity $40m in FY22-FY24 (including c. $15m delivered in FY22) Inflation expected to be largely offset by productivity	No change
Growth	Targeted organic and inorganic growth for Medibank Health and Health Insurance remain areas of focus, supported by a strong capital position	No change
Financial impacts of cybercrime event	N/A	Based on our current actions in response to the cybercrime event, we currently estimate $25m-$35m pre-tax non-recurring costs will impact earnings in 1H23. These non-recurring costs do not include further potential customer and other remediation, regulatory or litigation related costs. This cybercrime event continues to evolve and at this stage, we are unable to predict with any certainty the impact of any future events on Medibank including the quantum of any potential customer and other remediation, regulatory or litigation related costs.