HELM ADVISORY

November 2022

Communique

Welcome to our November newsletter as we enjoy the cricket, horse racing and hopefully some more sunshine. Our thoughts go out to the flood-savaged communities in the Eastern States.

DON'T FORGET TO APPLY FOR YOUR DIRECTOR IDENTIFICATION NUMBER (DIN)

All directors appointed under the Corporations Act 2001(Cth) are required to have a DIN by 30 November 2022 if they were appointed as directors before 31 October 2021. This is the looming deadline for most directors who have been in the job for over a year.

For those directors appointed between 1 November 2021 and 4 April 2022, they needed to apply within 28 days of appointment.

For new directors from 5 April 2022, they need to apply before their appointment.

If you cannot apply by the due date then you need to complete an application for an extension of time to apply for a DIN. It is a criminal offence if you do not apply on time.

There is no current requirement to provide your DIN to either ASIC or the companies to which you are a director. You still need to advise your company of any change in address or other details so that the company can update the public record.

There are now four new director ID offences in the Act which come under ASIC's enforcement division:

1. S1272C Failure to have a DIN when required to do so;
2. S1272D Failure to apply for a DIN when directed by the Registrar;
3. S1272G Applying for multiple DINs; and
4. S1272H Misrepresenting a DIN.

Penalties for breaches of the first two sections listed above include a maximum criminal penalty of $13,200 and a maximum civil penalty of $1.1m for an individual.

Penalties for breaches of the second two sections listed above include a maximum criminal penalty of $26,640. One year imprisonment or both and a maximum civil penalty of $1.1m.

So please ensure that your clients register for the DIN to avoid any penalties. As you can see the penalties are quite large.

Visit the ABRS website for more information and to apply:www.abrs.gov.au/director-identification-number

WHEN DO DIRECTORS OWE A DUTY OF CARE TO CREDITORS?

Until recently, directors of a solvent company owed a duty of care to the company and its shareholders.

A recent case in the UK Supreme Court, BTI 2014 LLC v Sequanan SA and others [2022] UKSC 25, confirmed that directors owed a duty of care to creditors under common law and equity where there is either imminent insolvency or there is the probability of an insolvent liquidation or administration that the directors know or ought to know.

In this case, the company did not enter into insolvency for nine years after the distribution of a significant dividend to shareholders so directors were found to have not breached any duty owed to the company or its creditors. The insolvency was not imminent.

As Australia has derived much of its corporate law from the UK, it is likely that our courts would follow this judgment made by their Lordships in the highest court in the UK. Notably, the duty of care to creditors is not to be enlivened where there is a temporary cashflow deficit. Their Lordships stated that the duty to creditors arises out of common law rather than a statutory duty which makes the case particularly useful for Australia.

CYBER ATTACKS

Recent news of cyber attacks at Optus and Medibank have rocked the confidence of the Australian public in providing confidential and private details to these large public companies. Both companies have been criticised for their poor communication of the cyber attack with their customers.

In the case of Optus, not only the personal data of current customers were disclosed but former customers as well. Passport details and driver's licence details were among some of the personal information that was stolen. Luckily, NSW had introduced a two-stage identification process with their driver's licences which meant that the cyber thieves were unable to use the data without the card number on the licence.

Originally Medibank revealed that the cyber attack was limited to its budget insurance sub-brand, AHM and data collected about international students studying in Australia who use Medibank under its OSHC service. More recently, Medibank has revealed that its main brand was also attacked and stolen customer data was from all three entities. It is believed that the hackers stole the credentials of someone who had high-level access within the Medibank computer systems which allowed them to infiltrate the computer network.

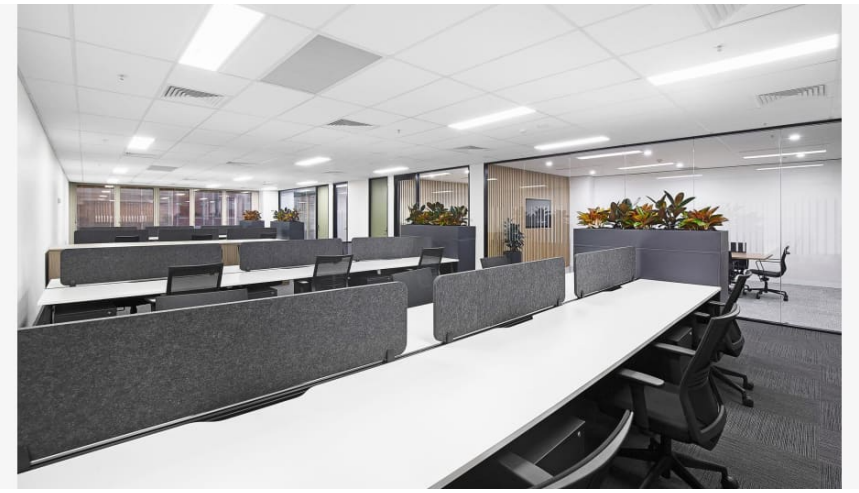
Even an online cyber security conference held by the Australian Institute of Company Directors was recently hacked and participants trying to log in them tried to use the online chat. A link was posted on the online chat requesting credit card details for a fake Eventbrite link.

The online conference was subsequently cancelled. It is unknown whether any of the participants entered in their credit card details and had them stolen.

Clearly, it is time for these large companies to invest in higher level cyber security to protect their customer's private information that they hold on their databases otherwise these breaches will become more common.

The Federal government is to introduce legislation to increase the penalties for repeated and serious privacy breaches from $2.2m to the greater of $50m, three times the value of any benefit obtained through the misuse of information or 30% of a company's adjusted turnover in the relevant period. In addition, the Australian Information Commissioner has been provided with additional of strengthened powers in the Bill.

HELM ADVISORY IS MOVING OFFICES



Our team is being relocated to brand new office space on level 6 of the OCBC Building, 75 Castlereagh Street Sydney. You will still be able to contact us on the usual emails and telephone numbers but drop in and check them out anytime after 5 December 2022. We are closer to the Courts and right near Centrepoint.

We can help you now

If you have clients who are experiencing difficulty in paying their debts and/or need to restructure their business, please contact me.

Stephen Hathway

0413 443 224

Philip Hosking

0434 407 748

Bob Pfaff

0405 506 040

Shijun Chan

0413 986 778

Bruce Hyunh

0402 662 982

Helm Advisory

Suite 2 Level 16, 60 Carrington Street Sydney