Heat's Cyber-attack
Current employees and ex-employees should be on the alert

Heat was subjected to a cyber-attack in February, which may have resulted in the personal information we have on electronic file for current employees and ex-employees being compromised – including, potentially, information such as your bank account details, name, address, next of kin, date of birth and tax file number. By now, you should have received a letter from us advising you of this.

I am so relieved to say that, in the months since the cyber-attack, we have not received any reports of suspicious activity on any Heat employees, or ex-employees, accounts or TFNs. However, we do advise you to continue to be vigilant in monitoring your personal banking and credit cards.

I am also pleased to tell you that that our business systems team has undertaken significant work to fortify our systems against future attacks and that this is proving extremely effective. Late in March, the Australian Cyber Security Centre (a department of the Australian Defence Force) shared with us that they had received advice from the UK National Crime Authority that a malicious cyber actor was selling access to the Heat Group network on dark web forums. We have had at least 15 attempts per day to enter our systems again so we can see the impact of this. But, because of the way our systems have been rebuilt and fortified since the attack, these attempts to breach our network have been ineffective.

The ACSC also told us how many other large enterprises had been victims of the same malicious cyber actor. Unfortunately, this is part of our landscape now and all of us – businesses and individuals alike – need to develop and maintain a higher level of vigilance than ever before.

I have some further information that I would like to share with you too:

- The Office of the Australian Information Commissioner (OAIC) has outlined the kinds of steps that individuals can take to reduce their risk of harm following a data breach on their website: https://www.oaic.gov.au/individuals/data-breach-guidance/what-to-do-after-a-data-breach-notification

- If you haven't do so already, the OAIC also recommend that you report this to the ATO's Client Identity Support Centre, in order that it can monitor any unusual or suspicious TFN activity: https://www.ato.gov.au/Individuals/Tax-file-number/Lost-or-stolen-TFN

If you have any questions or concerns, do not hesitate to reach out to me.

Best regards,

Gillian Franklin
Founder and Managing Director