Latitude Group Holdings Ltd
ACN 604 747 391

Level 18, 130 Lonsdale St,
Melbourne VIC 3000

latitudefinancial.com

27 March 2023

ASX ANNOUNCEMENT

Cybercrime update

From the outset of the cyber-attack on Latitude (ASX: LFS), we have sought to keep our customers, partners, employees and the broader community as up to date as we can.

This malicious attack on Latitude is under investigation by the Australian Federal Police and we continue to work with the Australian Cyber Security Centre and our expert cyber-security advisers.

To the best of our knowledge no suspicious activity has been observed in Latitude's systems since Thursday 16 March 2023.

As our forensic review continues to progress, we have identified that approximately 7.9 million Australian and New Zealand driver licence numbers were stolen, of which approximately 3.2 million, or 40%, were provided to us in the last 10 years.

In addition, approximately 53,000 passport numbers were stolen.

We have also identified less than 100 customers who had a monthly financial statement stolen.

We will reimburse our customers who choose to replace their stolen ID document.

A further approximately 6.1 million records dating back to at least 2005 were also stolen, of which approximately 5.7 million, or 94%, were provided before 2013.

These records include some but not all of the following personal information: name, address, telephone, date of birth.

Latitude maintains insurance policies to cover risks, including cyber-security risks, and we have notified our insurers in respect of this incident.

We recognise that today's announcement will be a distressing development for many of our customers and we apologise unreservedly.

We are writing to all customers, past customers and applicants whose information was compromised outlining details of the information stolen and our plans for remediation.

Supporting our customers

Latitude is undertaking a comprehensive customer care program to support affected individuals. Some of the steps we are taking include:

Latitude's dedicated contact centres are available for affected customers in Australia and New Zealand between 9am – 6pm AEDT/NZST, Monday – Friday.

Hardship support is available via our dedicated contact centres for customers who are in a uniquely vulnerable position as a result of this cyber-attack.

We have engaged IDCARE, a not-for profit organisation specialising in providing free, confidential cyber incident information and assistance. If you wish to speak with one of their expert Case Managers, please visit idcare.org or call (New Zealand) 0800 121 068, 11am – 6pm NZST, Monday – Friday (excluding public holidays) or (Australia) 1800 595 160 (use the referral code LAT23).

Mental Health and Wellbeing Support is available free of charge through our Support Line 0800 808 374 (New Zealand) or 1800 808 374 (Australia).

The help page on our website is also being kept up to date with the latest information.

For personal use only

Steps you can take to protect yourself

There are immediate precautions that you can take, which include:

- Contacting one of Australia's credit reporting agencies for a credit report so you can check if your identity has been used to obtain credit without your knowledge.

- In New Zealand, checking your credit record to confirm if your identity has been used to obtain credit without your knowledge. For further information, please refer to: govt.nz/browse/consumer-rights-and-complaints/debt-and-credit-records/check-your-own-credit-report

- Requesting the credit reporting agencies to place a credit ban or suspension on your credit file via their website or by contacting them directly. Please be aware that you will not be able to apply for credit while the ban or suspension is in place.

Be Alert

We urge our customers to be vigilant with all online communications and transactions, including:

- Staying alert for any phishing scams via phone, post or email
- Ensuring communications received are legitimate
- Not opening texts from unknown or suspicious numbers
- Changing passwords regularly with 'strong' passwords, not re-using passwords and activating multi-factor authentications when available on any online accounts
- Latitude will not contact customers asking for password or sensitive information

If you are a victim of cybercrime, you can report it at ReportCyber on the Australian Cyber Security Centre website.

If you wish to report a scam or a vulnerability, go to ScamWatch.

Latitude Financial CEO Ahmed Fahour said:

"It is hugely disappointing that such a significant number of additional customers and applicants have been affected by this incident. We apologise unreservedly.

"We are committed to working closely with impacted customers and applicants to minimise the risk and disruption to them, including reimbursing the cost if they choose to replace their ID document. We are also committed to a full review of what has occurred.

"We urge all our customers to be vigilant and on the look-out for suspicious behaviour relating to their accounts. We will never contact customers requesting their passwords.

"We continue to work around the clock to safely restore our operations. We are rectifying platforms impacted in the attack and have implemented additional security monitoring as we return to operations in the coming days.

"We thank customers and merchant partners for their support and patience. Customers can continue to make transactions on their Latitude credit card."

Authorised for release to the ASX by the Board of Directors.

For further information:

Media
Mark Gardy
+61 412 376 817

Investor Relations
Matthew Wilson
+61 401 454 621

For personal use only