Latitude Group Holdings Ltd
ACN 604 747 391

Level 18, 130 Lonsdale St,
Melbourne VIC 3000

latitudefinancial.com

20 March 2023

ASX ANNOUNCEMENT

Cybercrime update

Latitude Financial (ASX: LFS) announced on 16 March 2023 that it had detected unusual activity on its systems which it can now confirm as a sophisticated, well-organised and malicious cyber-attack which remains active.

We recognise the distress to our customers caused by the theft of their personal information and we are committed to transparently updating our customers, partners, employees and the broader community.

Latitude immediately engaged leading external cyber security experts, the Australian Cyber Security Centre, the Australian Federal Police and other relevant Government agencies.

The attack on Latitude is now the subject of an investigation by the Australian Federal Police.

Our people are working around the clock to contain the attackers. We have taken the prudent action of isolating some of our technology platforms which means that we are currently not onboarding new customers.

Because the attack remains active, we have taken our platforms offline and are unable to service our customers and merchant partners. We cannot restore this capability immediately, however we are working to do so gradually over the coming days and ask our customers for their continued patience. Our restoration of these services is aligned to our forensic review.

In conjunction with our cyber-security experts, we are continuing our forensic review of our IT platforms to identify the full extent of the theft of customer information as a result of the attack on Latitude.

So far, Latitude can confirm that:

- As previously disclosed, approximately 330,000 customers and applicants have had their personal information stolen
- Approximately 96% of the personal information stolen was copies of drivers' licences or driver licence numbers
- Less than 4% was copies of passports or passport numbers
- Less than 1% was Medicare numbers

As our review deepens to include non-customer originating platforms and historical customer information, we are likely to uncover more stolen information affecting both current and past Latitude customers and applicants. We will provide a further update when we have more information to share.

Latitude encourages our customers to remain vigilant. We will never contact customers requesting their passwords.

From today, Latitude will commence contacting customers and applicants who have so far been impacted by this criminal act, having already written to all our customers on Thursday 16 March 2023 to alert them to the cyber-attack.

Latitude will confirm to each impacted customer and applicant what personal information has been stolen, what we are doing to support them and what additional steps customers should consider taking to further protect their information. This includes Latitude working with relevant agencies to replace identification documents, where necessary, at no cost to our customers.

We have engaged IDCARE to help support those impacted. IDCARE is a not-for profit organisation and Australia and New Zealand's national incident response service specialising in providing free, confidential cyber incident information and assistance. Impacted customers and applicants will be able to contact IDCARE during business hours on 1800 595 160.

As of today, Latitude has established dedicated contact centres for impacted customers in Australia and New Zealand to answer queries, as well as a dedicated help page on our website to keep customers and partners fully

informed of developments.

Once the cyber-attack is contained, Latitude commits to a review of this incident. This review will help Latitude to most effectively safeguard our customers, partners and platforms, while contributing to the continued fight against cyber-crime on Australian businesses.

Latitude is still assessing the anticipated total cost to it of this incident, including the cost to Latitude of the support we intend to provide our customers as described in this announcement.

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

Latitude Financial Services CEO Ahmed Fahour said:

"I sincerely apologise to our customers and partners for the distress and inconvenience this criminal act has caused. I understand fully the wider concern that this cyber-attack has created within the community.

"Our focus is on protecting the ongoing security of our customers, partners and employees' personal and identity information, while also doing everything we can to support customers and applicants who have had information stolen.

"While we continue to deliver transactional services, some functionality has been affected resulting in disruption. We are working extremely hard to restore full services to our customers and merchant partners and thank them for their patience and support. We understand their frustration. Customers should refer to Latitude's website for regular updates."

Authorised for release to the ASX by the Company Secretary, Vicki Letcher.

For further information:

Media
Mark Gardy
+61 412 376 817

Investor Relations
Matthew Wilson
+61 401 454 621

Latitude strongly advises all Australian and New Zealand citizens to regulary change passwords of important financial accounts.

There are immediate precautions that you can take to protect your identity and personal information:

1. You can contact one of Australia's three credit reporting bodies to obtain your credit report so you can confirm if your identity has been used to obtain credit without your knowledge.

   You can also request the credit reporting bodies to place a credit ban on your credit file via their website or by contacting them directly. If you intend to apply for a credit ban, please be aware that you will not be able to apply for credit while the ban is in place.

Credit Reporting Body	Contact Information	Website
Illion	AU – 1300 734 806 NZ – 0800 733 707	illion.com.au illion.co.nz
Equifax	AU – 138 332 NZ – 0800 692 733	equifax.com.au equifax.co.nz
Experian	AU – 1300 783 684	experian.com.au
Centrix	NZ – 0800 236 874	centrix.co.nz

2. You can refer to Australian Government information on how you can protect yourself at cyber.gov.au or to Office of the Privacy Commissioner for information on how you can protect yourself at privacy.org.nz

3. You should be alert for any phishing scams that may be sent via SMS, phone, email or post.

4. You should always verify the sender of the communications you receive to ensure they are legitimate.

5. You should never click on links contained in SMS or email messages unless you know they are legitimate.

6. You should be careful when opening or responding to texts from unknown or suspicious numbers.

7. You should be careful when answering calls from private numbers or callers originating from unusual geographic locations.

8. You should regularly update your passwords and ensure you are using strong passwords. Also use multi-factor authentication where possible.