T: +44 (0)20 3320 5000
finastra.com

Finastra Group Holdings Ltd
4 Kingdom Street,
Paddington,
London, W2 6BD

3 April 2020

Finastra Statement on Cyberattack

As many of our customers will be aware, Finastra was recently targeted in a cyberattack. As a result of this, on 20th March, we took certain proactive steps to protect our systems and our customers' data, which meant that we had to interrupt service to some customers. First and foremost, we would like to apologize to all affected customers for the inconvenience and concern that this delinquent attack has caused to them and, in turn, their own customers.

In recent weeks the world has seen the number and intensity of cyberattacks increase significantly across all sectors of industry, sadly including even the medical and not-for-profit sectors. These attacks have been deliberately timed to capitalize on the challenges we all face in protecting our colleagues and loved ones from COVID-19. Unfortunately, cyberattacks remain a constant threat for everyone, and we all need to continue to guard against this.

In terms of the incident itself:

- Our security systems were able to detect a malware attack that had all the hallmarks of an eventual ransomware attack; as such our security protocols were quickly deployed.
- We promptly engaged a leading independent forensic firm to help investigate the scope of the incident and assist with securing our systems.
- Based on their advice, we made the decision to temporarily disconnect our servers from external traffic in order to deny the threat actor any possible access while we conducted a thorough investigation and put any necessary remediation plans in place.

Our decision to disconnect the relevant US data center servers mainly affected certain North American customers. We did not take this decision lightly, but we will always put the security of our customers—and their customers—as our absolute priority. Customers running our software in their own environments were not affected.

In terms of the effects of the attack:

- Throughout our investigation to date, we have not detected any compromise to either applications or their related data. Neither do we have any evidence that any customer data was accessed or exfiltrated, nor that any of our customers' networks were in any way impacted.
- Since remediation plans were activated, we have been progressively reconnecting our systems to outside traffic.
- As of today, all of our systems are now available for customer reconnection and, together with our specialist forensic advisors, we have not detected any further ongoing issues associated with the cyberattack.

In terms of remediation:

- We are putting in place a range of additional measures to combat increased cyberattack activity. These include, together with external specialist teams, deploying a leading forensic platform to all Finastra endpoints to actively monitor, detect, analyze and respond to any threat on an ongoing 24x7 basis.

Once again, Finastra would like to apologize for any impact this incident may have had on its customers. It has been encouraging to see that the world-wide restrictions currently in place due to COVID-19 have not materially hampered our ability to respond to the incident, and we would like to reassure our customers of our utmost support. Like many companies, we have activated our global pandemic contingency plans and, with these in place, we are continuing to work with all of our customers across the globe. We appreciate your support and anticipate providing our next update on 17th April.