T: +1 800 989 9009
finastra.com

FINASTRA
744 Primera Boulevard,
Suite 2000, Lake Mary,
FL 32746
United States

March 25th, 2020

Re: Cyber Incident Status Update

To Whom it May Concern,

Following last week's cyberattack, I'm sharing with you an update on our progress to date. I hope that it addresses any concerns or queries you may have at this time – be assured that we are providing all the information that we possibly can, as we continue to work to bring all of our products and services back online and into production. If you have any further questions, please contact your account team and we will keep you updated as quickly and transparently as possible.

Origin of the attack

Through proactive network monitoring, our IT security and risk teams successfully detected an unknown actor on our network. At this time, we believe the attack originated in a US datacenter, and appears to have intended to disrupt our network by deploying a ransomware attack. Many of you are interested in the origin (location) and type of attack (malware), but due to the ongoing investigation, we are unable to share this level of detail at the moment. We are committing significant resources to investigating the source of this attack and will continue to update you as soon as we are able.

Timeline of containment

As soon as the intrusion was detected, we began work to contain it. We brought in leading cybersecurity partners, to assist us with investigating, containing and mitigating the threat. Overnight on Thursday (Eastern Time) we made the difficult, but necessary, decision to temporarily disconnect our servers from external traffic, to deny the unknown actor access while we conducted a thorough review.

Was any data breached?

At this time, **we have no evidence that any customer data was accessed or exfiltrated, nor do we believe our clients' networks were impacted**. No customers running software in their own environments were affected. We believe that by moving rapidly and taking these proactive but extreme

© Finastra 2019
All rights reserved

measures, we were able to successfully contain the threat, secure our network and protect our clients' data.

Are all services back online?

We had to (and continue to) bring systems back online in a controlled, secure, and systematic way. The majority of our systems and servers are now back online, having been through rigorous security testing, and we are currently working with our partners to ensure that third-party services are subject to the same critical security reviews as our proprietary systems.

What was the attack vector?

At the current time, we are working with our security partners to ascertain the vulnerability that allowed this threat into the network. Our investigation is still ongoing but are taking a number of additional protective measures to bolster our security. In addition to a forensic review of all our network security systems and protocols, we have implemented additional threat detection and protection capabilities, across our network and endpoint devices.

We appreciate your ongoing support during this time, as we get back to full service availability. This attempt came about as we – like much of the world – were focused on emergency measures to move our workforce to full remote working, whilst continuing to run operations without disruption. However, we are confident that we acted swiftly to mitigate the risk to you, our valued customers. The whole Finastra team remains committed to continuing to provide you with the tools, systems and services that deliver on your goals, albeit remotely, during these extraordinary times.

Thank you, and best wishes,

Finastra Leadership Team