We have concluded our investigation into the January 2022 compromise of our third-party vendor.

At the outset of our investigation, we focused on a five-day window of time, between January 16 and 21, when the third-party forensic firm, engaged by our vendor Sitel, indicated that the threat actor had access to their environment. Based on that window of time, we determined that the maximum potential impact of the incident was 366 Okta customers whose tenants were accessed by any Sitel customer support engineer within that time.

As a result of the thorough investigation of our internal security experts, as well as a globally recognised cybersecurity firm whom we engaged to produce a forensic report, we are now able to conclude that the impact of the incident was significantly less than the maximum potential impact Okta initially shared on March 22, 2022.

The final forensic report of the globally recognised cybersecurity firm we engaged concluded that:

* The threat actor actively controlled a single workstation, used by a Sitel support engineer, with access to Okta resources.
* Control lasted for 25 consecutive minutes on January 21, 2022.
* During that limited window of time, the threat actor accessed two active customer tenants within the SuperUser application (whom we have separately notified), and viewed limited additional information in certain other applications like Slack and Jira that cannot be used to perform actions in Okta customer tenants.
* The threat actor was unable to successfully perform any configuration changes, MFA or password resets, or customer support “impersonation” events.
* The threat actor was unable to authenticate directly to any Okta accounts.

While the overall impact of the compromise has been determined to be significantly smaller than we initially scoped, we recognise the broad toll this kind of compromise can have on our customers and their trust in Okta.