Altair Engineering Inc.
1820 E Big Beaver Road
Troy, Michigan 48083

July 11, 2023

Division of Corporation Finance
Office of Technology
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Attn: Edwin Kim, Esq. and Mitchell Austin, Esq.

Re: Altair Engineering Inc.
Form 10-Q for the Fiscal Quarter Ended March 31, 2023
Filed May 4, 2023
File No. 001-38263

This letter is submitted by Altair Engineering Inc. ("Altair") in connection with the Staff's comment letter dated June 12, 2023. We appreciate the Staff's taking the time to discuss its comment with our Chief Legal Officer and outside counsel on June 19, 2023 and the Staff's agreement to extend the date on which a response is due until July 12, 2023.

The Staff's comment has been retyped below in italics, and is followed by our response:

SEC Comment:

Form 10-Q for the Fiscal Quarter Ended March 31, 2023

General

1. *We note that you reported a data breach to the Commonwealth of Massachusetts in 2022, as discussed here: https://www.mass.gov/doc/data-breach-report-2022/download. However, your periodic reports, including this Form 10-Q and your Form 10-K for the fiscal year ended December 31, 2022, only include risk factor disclosure stating that you may experience cyber-attacks and other security incidents. In light of the data breach, please update this risk factor language that characterizes this risk as potential or hypothetical to note that you have experienced a data breach and describe it as necessary. Additionally, please tell us whether you believe this data breach was material and explain how you reached this conclusion. Lastly, consider updating your discussion of how your board administers its risk oversight function in overseeing cybersecurity risks. For additional guidance, consider the Commission Statement and Guidance on Public Company Cybersecurity Disclosures (SEC Release No. 33-10459), available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.*

Altair's Response:

On November 8, 2021, Altair identified a malicious cybersecurity incident performed by an unknown third-party. Promptly upon detection of the security incident, Altair implemented its incident response plan to assess, contain and mitigate the incident and to commence a forensic investigation.

Within four hours of the incident, Altair's cybersecurity defense system and IT security team determined that certain servers and workstations in Altair's environment had been infected with malware, and affected servers were shut down to contain the threat. In addition, the IT security team switched off VPN access, disconnected cloud communications, and shut down machines that hosted backups and mass storage servers.

Within 24 hours, Altair engaged a cybersecurity forensic firm, legal counsel and other incident response professionals. Shortly after the forensic firm was engaged, the forensic firm assisted Altair in (i) determining the scope of the threat, including the type of attack, environments affected, possible user accounts compromised, and known infected machines, and (ii) gradually restoring functionality to impacted machines and environments.

Promptly after management made a preliminary assessment, this matter was reported to Altair's Board of Directors. The Board of Directors, in turn, discussed this matter at a regularly scheduled meeting approximately eight days after the incident was identified.

In the following months, Altair worked to further strengthen its IT security environment to provide additional protections against future cybersecurity incidents. In addition, at the conclusion of a fulsome review of all data impacted by the incident, Altair disclosed the event to applicable law enforcement and government agencies, including to the Commonwealth of Massachusetts as noted by the Staff in its Comment Letter.

Materiality Determination

Altair believes the cybersecurity incident was not material. Altair considered the materiality of the cybersecurity incident at the time of the incident, in its review with its Board of Directors eight days after the incident was discovered and during the period leading up to the filing of its Annual Report on Form 10-K for the year ended December 31, 2021. Factors considered included the factors noted by the Commission in its Statement and Guidance on Public Company Cybersecurity Disclosures, as referenced by the Staff in its Comment Letter. Altair concluded at those times, as it respectfully concludes at this time, that the cybersecurity incident did not have a material impact on Altair, either from an operational perspective, a financial statement perspective or a preparedness perspective.

More specifically, with respect to operations:

- Net expenses to remediate the incident were negligible, amounting to less than $200,000.
- Business with our customers continued uninterrupted, including engaging in new and ongoing sales opportunities, performance of our products and services, customer support, invoicing, and collections. Altair did not lose revenues or fail to retain or attract customers as a result of the cybersecurity incident.
- Altair did not incur net expenses to provide incentives to customers or business partners in order to maintain our relationships with those entities.
- Altair did not suffer reputational damage at the time of the incident or, with the benefit of hindsight, at any time during the more than 18 months subsequent to the incident, relating in any way to the incident.
- Altair did not suffer any damage to its competitiveness, stock price or long-term shareholder value relating in any way to the incident.
- No litigation resulted from the cybersecurity incident.
- Altair did not experience a material increase to its cybersecurity insurance premiums as a result of the cybersecurity incident.
- While steps were taken subsequent to the incident to upgrade Altair's networks and enhance cybersecurity protection in order to mitigate the risk of future cybersecurity incidents, those steps were consistent with Altair's ongoing focus on cybersecurity and were well within Altair's normal operating budgets.
- As noted above and by the Staff in its Comment Letter, Altair notified applicable regulatory authorities. No follow-up actions were taken by any such authorities.

With respect to our financial statement analysis:

- The cybersecurity incident occurred during Altair's fourth fiscal quarter on November 8, 2021, which was four days after Altair had issued its revenue and profitability projections for the fourth quarter on November 4, 2021. Revenue and profitability were not impacted by the cybersecurity incident, and Altair exceeded its revenue and profitability projections for the fourth quarter, as disclosed in the earnings release issued on February 24, 2022.
- As noted above, net remediation expenses were negligible, including for legal and other professional services related to the incident, and enhanced cybersecurity protection expenses were within anticipated operating budgets.

- Altair did not experience any claims related to warranties, breach of contract, product recall/replacement or indemnification of counterparties.
- As noted above, Altair did not experience a material increase to its cybersecurity insurance premiums.
- In connection with the incident, Altair did not experience diminished future cash flows, impairment of intellectual, intangible or other assets, recognition of material liabilities, or increased financing costs.

From a preparedness standpoint, Altair has considered both its disclosure controls and its internal controls. With respect to disclosure controls, we believe that the controls operated as they should have operated: Altair's senior management was contacted on the date of the incident, enabling Altair to commence implementing its incident response plan that day. As noted above, Altair's Board of Directors was promptly notified and discussed the incident at its regularly scheduled meeting approximately eight days after the incident was identified. In addition, inside and outside counsel were involved throughout this process to ensure Altair's compliance with applicable laws and regulations. With respect to internal controls, Altair concluded that its ability to respond promptly in real time, its ability to remediate and mitigate risks in a reasonable time frame, and the strength of Altair's overall cybersecurity controls provided strong assurance that our internal controls were and are effective.

Disclosure

With respect to the cybersecurity disclosures in Altair's most recent Annual Report on Form 10-K, please note that in addition to the risk factor disclosure identified by the Staff, Altair also included the following disclosure in Item 1 of its 10-K:

> **"Information technology and cybersecurity**
>
> Our business and support functions utilize information systems that provide critical services to our employees and customers. Led by our Chief Information Security Officer, our team of professionals manage and support our communication platforms, transaction-management systems, and analytics and reporting capabilities. We use both third-party cloud services and off-site, secure data centers in North America and Europe for our core applications.
>
> Information security and privacy are important concerns, with an escalating cyber-threat environment and evolving regulatory requirements driving continued investment in this area. We continue to evaluate and assess our systems in the changing regulatory environment.

We have in place, and seek to continuously improve, a comprehensive system of security controls, managed by a dedicated staff. Periodically, we engage the services of third parties to perform security penetration testing and may update our security controls in response. We also provide our staff with regular security risk awareness, education, and training. Despite these efforts computer viruses, hackers, employee misuse or misconduct, and other internal or external hazards including natural disasters could expose our data systems to security breaches, cyber-attacks, or other disruptions.

We have incident response and business continuity plans for our operations. Our recovery plans include arrangements with our off-site secure data centers and cloud infrastructure. We believe we will be able to utilize these plans to efficiently recover key system functionality in the event that our primary systems are unavailable."

Altair understands that the Staff has questioned whether Altair's existing risk factor language, referencing incidents that "may occur", could lead investors to conclude that Altair has never experienced any cybersecurity incidents, including incidents that are not material enough to warrant disclosure. That certainly was not Altair's intention. Our belief is that our investors, as well as potential investors, read Altair's cybersecurity risk factor to learn what may disrupt Altair materially in the future. Respectfully, we do not believe that the historical occurrence of a non-material cybersecurity incident occurring 18 months ago has any bearing on whether Altair will experience any material cybersecurity incidents in the future.

If Altair were required to disclose that it experienced a cybersecurity incident that was not material, it would be making a disclosure that is not contemplated by the guidance provided by the Staff or by the SEC's pending rule proposal regarding cybersecurity disclosures. That guidance and the proposed rule mandate disclosure only when cybersecurity incidents are material. A requirement for Altair to disclose a non-material event would place Altair in a different position than other issuers, which are not required to disclose non-material cybersecurity incidents that they have experienced. This different treatment could adversely impact Altair and its investors.

As is the case with all other public companies, Altair regularly makes materiality determinations. We take that responsibility very seriously, but with the understanding that if a matter does not meet the materiality threshold, it need not be disclosed. We believe that prudent investors understand and appreciate that issuers focus their disclosures on material matters. We also believe that prudent investors understand that the absence of a disclosure regarding a particular matter (*e.g.*, litigation) does not mean that insignificant matters (*e.g.*, a minor litigation matter) have not occurred.

Finally, we are also concerned that if Altair discloses this matter as an event that was not material, its investors may expect Altair to disclose other matters that do not meet the materiality threshold. That is not an expectation that we or any other issuer would want to create.

In light of the facts described herein regarding the lack of materiality of the cybersecurity incident and our comments regarding our disclosure obligations, we respectfully request that the Staff reconsider its request regarding the modification of our cybersecurity risk factor.

Board Oversight

In its Comment Letter, the Staff has also asked Altair to consider updating our discussion of how our Board administers its risk oversight function in overseeing cybersecurity risk. In preparing our next Annual Report on Form 10-K, we will consider this disclosure as part of our consideration of the SEC's proposed rule on cybersecurity incidents.

***

We believe that this letter fully responds to your Comment. However, if you have any questions or comments regarding the foregoing, please feel free to contact the undersigned at 248-614-2400, or our outside counsel, Kate Basmagian (212-262-6700) or Peter Ehrenberg (212-262-6700) of Lowenstein Sandler, LLP.

Very truly yours

ALTAIR ENGINEERING INC.

By: /s/ Matthew Brown
Name: Matthew Brown
Title: Chief Financial Officer

cc: Raoul Maitra, Esq.
Mr. Brian Gayle
Kate Basmagian, Esq.
Peter Ehrenberg, Esq.