Cooley

Jon C. Avina
T: +1 650 843 5307
javina@cooley.com

***FOIA Confidential Treatment Request**
Confidential Treatment Requested by Confluent, Inc.
in connection with its Registration Statement
on Form S-1 filed on June 1, 2021

VIA EMAIL AND EDGAR

June 23, 2021

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

Attn: Jan Woo, Legal Branch Chief
Alexandra Barone, Staff Attorney
Stephen Krikorian, Accounting Branch Chief
Morgan Youngwood, Senior Staff Accountant

Re: Confluent, Inc.
Registration Statement on Form S-1
Filed June 1, 2021
File No. 333-256693

Ladies and Gentlemen:

On behalf of Confluent, Inc. (the "***Company***"), we are providing this letter in response to verbal comments (the "***Comments***") received from the staff of the U.S. Securities and Exchange Commission's Division of Corporation Finance (the "***Staff***") on June 22, 2021 (the "***Comment Letter***") with respect to the Company's Registration Statement on Form S-1, filed on June 1, 2021 and amended on June 16, 2021 (the "***Amended Registration Statement***"). Set forth below are the Company's responses to the Comments. Page references in the text of the Company's responses correspond to the page numbers of the Amended Registration Statement.

Due to the commercially sensitive nature of certain information contained in this letter, the Company hereby requests, pursuant to 17 C.F.R. §200.83, that certain portions of this letter be maintained in confidence, not be made part of any public record, and not be disclosed to any person. In accordance with 17 C.F.R. §200.83(d)(1), if any person (including any governmental employee who is not an employee of the Commission) should request access to or an opportunity to inspect this letter, we request that we be immediately notified of any such request, be furnished with a copy of all written materials pertaining to such request (including, but not limited to, the request itself) and be given at least 10 business days' advance notice of any intended release so that the Company may, if it deems it to be necessary or appropriate, pursue any remedies available to it. In such event, we request that you telephone the undersigned at (650) 843-5307 rather than rely on the U.S. mail for such notice.

* * *

Verbal Comments Relating to the Cybersecurity and Data Privacy Risk Factor

In response to Comments received from the Staff regarding the Company's risk factor set forth on pages 42 through 43 of the Amended Registration Statement relating to cybersecurity and data privacy matters, the Company respectfully submits to the Staff the following revised risk factor for consideration, with additions marked with underlines and deletions marked as strikethrough text. The Company respectfully advises the Staff that it intends to include the revised risk factor in the Company's final prospectus relating to the Amended Registration Statement, to be filed pursuant to Rule 424(b) under the Securities Act of 1933, as amended.

Confluent, Inc. requests that the information contained in this letter, marked by brackets, be treated as confidential information pursuant to 17 C.F.R. §200.83.

"***If we or third parties who we work with experience a security breach, or if the confidentiality, integrity, or availability of our information technology, software, services, communications, or data is compromised, our offering may be perceived as not being secure, our reputation may be harmed, demand for our offering may be reduced, proprietary data and information, including source code, could be, and has in the past been, exfiltrated, and we may incur significant liabilities.***

Our offering involves the transmission and processing of data, which can include personal information and our or our customers' or other third parties' sensitive, proprietary, and confidential information. Security breaches compromising the confidentiality, integrity, and availability of this information could result from cyber-attacks, computer malware, viruses, social engineering (including phishing), ransomware, supply chain attacks, credential stuffing, efforts by individuals or groups of hackers and sophisticated organizations, including state-sponsored organizations, errors or malfeasance of our personnel, and security vulnerabilities in the software or systems on which we rely, including third-party systems. Such incidents have become more prevalent in our industry, particularly against cloud services, and may in the future result in the unauthorized, unlawful, or inappropriate access to, inability to access, disclosure of, or loss of the sensitive, proprietary, and confidential information that we own, process, or control, such as customer information and proprietary data and information, including source code. Additionally, due to the ongoing COVID-19 pandemic, certain functional areas of our workforce remain in a remote work environment and outside of our corporate network security protection boundaries, which imposes additional risks to our business, including increased risk of industrial espionage, phishing, and other cybersecurity attacks, and unauthorized access to or dissemination of sensitive, proprietary, or confidential information.

We also rely on third parties to operate our critical business systems and process the sensitive, proprietary, and confidential information that we own, process, or control, including customer information and proprietary data and information, including source code. These third parties may not have adequate security measures and could experience a security breach that compromises the confidentiality, integrity, or availability of the systems they operate for us or the information they process on our behalf. Cybercrime and hacking techniques are constantly evolving, and we or third parties who we work with may be unable to anticipate attempted security breaches, react in a timely manner, or implement adequate preventative measures, particularly given increasing use of hacking techniques designed to circumvent controls, avoid detection, and remove or obfuscate forensic artifacts.

While we have taken steps designed to protect the confidentiality, integrity, and availability of our systems and the sensitive, proprietary, and confidential information that we own, process, or control, our security measures or those of third parties who we work with have been, and could from time to time in the future be, breached or may otherwise not be effective against security threats. For example, beginning in January 2021, a malicious third party gained unauthorized access to a third-party vendor, Codecov, that provides a software code testing tool, potentially affecting more than a thousand of Codecov's customers, ~~including us,~~ which we refer to as the Codecov Breach. In April 2021, we were notified that we had been impacted by the Codecov Breach. Through our investigations, we ~~have~~ determined that the attackers leveraged a vulnerability in Codecov's software to gain access to credentials in our development environment, and thereby obtained unauthorized read-only access to, and copied to overseas IP addresses, the private Github repositories containing our source code and certain internal-use documents containing references to certain customers and ~~certain documents containing~~ other customer-related attributes ~~information~~. Upon learning of the breach, we took action to revoke Codecov's access and discontinued our use of the Codecov service, rotated all of our credentials identified as exposed by the Codecov compromise to prevent further unauthorized access, analyzed available logs to determine whether there was evidence that the exposed credentials were leveraged to gain access to Confluent systems or systems of our customers, enhanced monitoring of our environment to identify and respond to suspicious activity, and engaged a third-party forensics firm to assist in our investigation, response, and impact mitigation. While the attackers obtained access to certain customer-related references and information described above, we have not found any evidence of access to any customer data sent through or stored in our products, nor have we found any evidence that the attackers modified any of our source code or uploaded any malware or any other malicious code to our system. However, the full extent of the impact of this incident on our operations, products, or services is not yet known, and we cannot assure you that there will be no impact in the near term or at all. This incident or any future

incidents relating to the Codecov Breach could result in the use of exfiltrated source code to attempt to identify vulnerabilities in our offering, future ransomware or social engineering attacks, reduced market acceptance of our offering, injury to our reputation and brand, legal claims against us, and the diversion of our resources.

In addition, we do not control content that our customers transmit, process, and maintain using our offering. If our customers use our offering for the transmission or storage of personal information and our security measures are or are believed to have been breached, our business may suffer and we could incur significant liability. In addition, our remediation efforts may not be successful.

Any security breach or other incident that results in the compromise of the confidentiality, integrity, or availability of our systems or the sensitive, proprietary, or confidential information that we own, process, or control, or the perception that one has occurred, including the Codecov incident described above, could result in a loss of customer confidence in the security of our platform and damage to our brand, reduce the demand for our offering, disrupt business operations, result in the exfiltration of proprietary data and information, including source code, require us to spend material resources to investigate or correct the breach and to prevent future security breaches and incidents, expose us to legal liabilities, including litigation, regulatory enforcement and indemnity obligations, claims by our customers or other relevant parties that we have failed to comply with contractual obligations to implement specified security measures, and adversely affect our business, financial condition, and results of operations. We cannot assure you that the limitations of liability in our contracts would be enforceable or adequate or would otherwise protect us from liabilities or damages.

These risks are likely to increase as we continue to grow and process, control, store, and transmit increasingly large amounts of data.

Additionally, we cannot be certain that our insurance coverage will be adequate or otherwise protect us with respect to claims, expenses, fines, penalties, business loss, data loss, litigation, regulatory actions, or other impacts arising out of security breaches, or that such coverage will continue to be available on acceptable terms or at all. Any of these results could adversely affect our business, financial condition, and results of operations."

The Company supplementally advises the Staff that, while its internal investigation relating to the Codecov Breach [***], the Company remains subject to risks relating to such incident as described in the risk factor above. As a result, the Company has determined that disclosure of the [***] may unduly mitigate against the remaining risks relating to such incident and may be misleading.

Verbal Comment Relating to Contingency Disclosures

In response to the Comment received from the Staff relating to the Company's determinations regarding existence of a contingency, the Company respectfully advises the Staff that it continues to believe that, with respect to the Codecov Breach, the Company does not have a basis to make any disclosure of or accrual for a loss contingency since the possibility of a loss is remote. The Company advises the Staff that no claims have been made or threatened against the Company by customers impacted by the Codecov Breach or any other parties to date. As previously disclosed to the Staff, upon receiving notice of the Codecov Breach by the affected third-party vendor in April 2021, [***] As the Company's internal investigation is substantially complete and the Company is not aware of any claims brought or threatened against the Company at this time, the Company determined that the possibility of a loss is remote. Further, because the Company determined that there was no contingent liability associated with the Codecov Breach, the event did not, and is not expected to have a determinable significant effect on the Company's consolidated financial statements at the time of occurrence or on the future operations of the Company. As a result, the Company further concluded that it was not necessary to disclose the Codecov Breach as a subsequent event in its consolidated financial statements.

* * *

Confluent, Inc. requests that the information contained in this letter, marked by brackets, be treated as confidential information pursuant to 17 C.F.R. §200.83.

Please contact me at (650) 843-5307 with any questions or further comments regarding the Company's responses to the Staff's Comments. Thank you in advance for your attention to this matter.

Sincerely,

Cooley LLP

/s/ Jon C. Avina
Jon C. Avina

cc: Steffan Tomlinson, Confluent, Inc.
Melanie Vinson, Confluent, Inc.
Siana Lowrey, Cooley LLP
Milson Yu, Cooley LLP
John Savva, Sullivan & Cromwell LLP
Sarah Payne, Sullivan & Cromwell LLP

Confluent, Inc. requests that the information contained in this letter, marked by brackets, be treated as confidential information pursuant to 17 C.F.R. §200.83.