ROPES & GRAY LLP
PRUDENTIAL TOWER
800 BOYLSTON STREET
BOSTON, MA 02199-3600
WWW.ROPESGRAY.COM

January 14, 2022

VIA EDGAR

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

Attention: Tracie Mariner
Kevin Vaughn

Re: Zai Lab, Ltd.
Form 10-K for Fiscal Year Ended December 31, 2020
Response dated November 9, 2021
File No. 001-38205

Ladies and Gentlemen:

On behalf of Zai Lab, Ltd. (the "Company"), we provide the following responses to the comment letter from the staff of the Division of Corporate Finance, Office of Life Science (the "Staff") of the Securities and Exchange Commission (the "Commission") dated December 10, 2021 related to the Company's Annual Report on Form 10-K for the year ended December 31, 2020 (the "Form 10-K") and the Company's response dated November 9, 2021. To assist your review, we have presented the text of the Staff's comments in italics below. The responses and information described below are based upon information provided to us by the Company.

Form 10-K for Fiscal Year Ended December 31, 2020

Part I

Item 1. Business, page 1

1. *At the onset of Part 1, please disclose prominently that you are not a Chinese operating company but a Cayman Islands holding company that conducts its operations through wholly owned subsidiaries based in China and that investors will not hold direct investments in the Chinese operating companies. Your disclosure should acknowledge that Chinese regulatory authorities could disallow this structure, which would likely result in a material change in your operations and/or value of your ADSs, including that it could cause the value of such securities to significantly decline or become worthless.*

Response to Comment 1:

The Company acknowledges the Staff's comment and advises the Staff that it will provide prominent disclosure of such risks at the onset of Part 1 of the Company's Form 10-K for the year ending December 31, 2021. Unless there are changes in relevant law or regulations, or in interpretations thereof that would necessitate changes to the below, we will add the following disclosure at the onset of Part 1 of the Company's Form 10-K for the year ending December 31, 2021:

> We are not a Chinese operating company, but a holding company incorporated in the Cayman Islands. As a holding company, we conduct a substantial portion of our operations through wholly-owned subsidiaries based in China. Investors will not hold direct investments in our Chinese operating companies. In July 2021, the Chinese government provided new guidance on China-based companies raising capital outside of China, including through arrangements called variable interest entities, or VIEs. Currently, our corporate structure contains no VIEs, and the life sciences industry in which we operate is not subject to foreign ownership limitations in China. However, there are uncertainties with respect to the Chinese legal system and there may be changes in laws, regulations and policies, including how those laws, regulations, and policies will be interpreted or implemented. If, in the future, the Chinese government determines that our corporate structure does not comply with Chinese regulations, or if Chinese regulations change or are interpreted differently, the value of our ADSs or ordinary shares may decline in value or become worthless.

2. *We note your response to prior comment two and disclosure on your Form 10-Q for the quarterly period ending September 30, 2021 (the "2021 Q3 Form 10-Q") and reissue in part. On page 1 of the 2021 Q3 Form 10-Q under the heading "Usage of Terms," we note that you provide the domicile of each subsidiary. However, please expand your disclosure to include the entity (including the domicile) in which investors are purchasing their interest. In addition, we note your disclosure, on page 1, stating that references in the quarterly report on Form 10-Q to "Zai Lab," the "Company," "we," "us," and "our" refer to Zai Lab Limited, a holding company, and its subsidiaries, on a consolidated basis. However, we note you refer to Zai Lab Limited and its subsidiaries as the "Group" throughout the filing. Please revise your disclosure to be consistent throughout.*

Response to Comment 2:

The Company acknowledges the Staff's comment and advises the Staff that, in future filings, the Company will revise its disclosure to clarify the entities that it refers to throughout the filing and will revise the "Note on Company Usage of Terms" section of the Company's Form 10-K for the year ending December 31, 2021 as follows:

Note on Company-Usage of Terms

Unless the context requires otherwise, references in this Annual Report on Form 10-K to "Greater China" refers to mainland China, Hong Kong, Macau, and Taiwan and "China" refers to mainland China and references in this Annual Report on Form 10-K to "Zai Lab," the "Company," "we," "us," and "our" refer to Zai Lab Limited, a Cayman Islands holding company, and its subsidiaries, on a consolidated basis and references to "Zai Lab Limited" refer to Zai Lab Limited, a holding company. Zai Lab Limited is the entity in which investors are purchasing their interest.

Our operating subsidiaries comprise of Zai Lab (Hong Kong) Limited, domiciled in Hong Kong; Zai Auto Immune (Hong Kong) Limited, domiciled in Hong Kong; Zai Anti Infectives (Hong Kong) Limited, domiciled in Hong Kong; Zai Lab (Shanghai) Co., Ltd., domiciled in China; Zai Lab International Trading (Shanghai) Co., Ltd., domiciled in China; Zai Lab (Suzhou) Co., Ltd., domiciled in China; Zai Biopharmaceutical (Suzhou) Co., Ltd., domiciled in China; Zai Lab Trading (Suzhou) Co., Ltd., domiciled in China; Zai Lab (Taiwan) Limited, domiciled in Taiwan; Zai Lab (US) LLC, domiciled in the United States. Additionally, as of the date of this Annual Report on Form 10-K, Zai Auto Immune (Hong Kong) Limited and Zai Anti Infectives (Hong Kong) Limited have non-substantial business operations.

Item 1A. Risk Factors, page 61

3. *We note your response to prior comment three and your updated risk factor disclosure on page 50 of your 2021 Q3 Form 10-Q and reissue in part. Please address the following regarding your response to prior comment three:*

- *Please disclose the consequences to you and your investors if you inadvertently conclude that approvals are not required, or applicable laws, regulations, or interpretations change.*
- *Regarding your disclosure that you are required to get certain approvals from Chinese authorities before transferring certain scientific data abroad or to foreign parties, please revise to more clearly disclose whether have you have received all requisite permissions and whether any permissions have been denied.*

Response to Comment 3:

The Company acknowledges the Staff's comment and advises the Staff that it will update the disclosures to address the points above in the Company's Form 10-K for the year ending December 31, 2021. Unless there are changes in relevant law or regulations, or in interpretations thereof that would necessitate changes to the below, we will add the following risk factors in response to this comment three:

We are not currently required to obtain approval or prior permission from the China Securities Regulatory Commission (CSRC) or any other Chinese regulatory authority under the Chinese laws and regulations currently in effect to issue securities to foreign investors. However, as there are uncertainties with respect to the Chinese legal system and changes in laws, regulations and policies, including how those laws and regulations will be interpreted or implemented, there can be no assurance that we will not be subject to such requirements, approvals or permissions in the future. We are required to obtain approvals and permissions from Chinese authorities in connection with our general business activities currently conducted in China.

The Chinese government has exercised, and may continue to exercise, substantial influence or control over virtually every sector of the Chinese economy through regulation and state ownership. Our ability to operate in China could be undermined if our Chinese subsidiaries are not able to obtain or maintain approvals to operate in China. The central or local governments could impose new, stricter regulations or interpretations of existing regulations that could require additional expenditures and efforts on our part to ensure our compliance with such regulations or interpretations.

As of the date of this Annual Report on Form 10-K, we are not required to obtain approval or prior permission from the CSRC or any other Chinese regulatory authority under the Chinese laws and regulations currently in effect to issue securities to foreign investors. However, as there are uncertainties with respect to the Chinese legal system and changes in laws, regulations and policies, including how those laws, regulations, and policies will be interpreted or implemented, there can be no assurance that we will not be subject to such requirements, approvals or permissions in the future. We are required to obtain certain approvals from Chinese authorities in order to operate our Chinese subsidiaries. We are also required to obtain certain approvals from Chinese authorities before transferring certain scientific data abroad or to foreign parties or entities established or actually controlled by them.

If our Chinese subsidiaries do not receive or maintain approvals, inadvertently conclude that approvals needed for their business are not required or if there are changes in applicable laws (including regulations) or interpretations of laws and our Chinese subsidiaries are required but unable to obtain approvals in the future, then such changes or need for approvals (if not obtained) could adversely affect the operations of our Chinese subsidiaries, including limiting or prohibiting the ability of our Chinese subsidiaries to operate, and the value of our ADSs or ordinary shares could significantly decline or become worthless.

To operate our general business activities currently conducted in China, each of our Chinese subsidiaries is required to obtain a business license from the local counterpart of the State Administration for Market Regulation, or SAMR. Each of our Chinese subsidiaries has obtained a valid business license from the local counterpart of the SAMR, and no application for any such license has been denied.

The Regulations on Mergers and Acquisitions of Domestic Enterprises by Foreign Investors, or the M&A Rules, appear to require that offshore special purpose vehicles, controlled by Chinese companies or individuals formed for the purpose of seeking a public listing on an overseas stock exchange through acquisitions of Chinese domestic companies or assets in exchange for the shares of the offshore special purpose vehicles, obtain CSRC approval prior to publicly listing their securities on an overseas stock exchange.

Based on the Chinese laws and regulations currently in effect, we are currently not required to obtain pre-approval from the CSRC to conduct a public offering in foreign capital markets, subject to interpretation of the existing Chinese laws, regulations, and policies by the Chinese government authorities. However, there is uncertainty as to how the M&A Rules will be interpreted or implemented by Chinese government agencies, including the CSRC. Additionally, new laws, rules and regulations or detailed implementations and interpretations of new or existing laws, rules, or regulations relating to the M&A Rules by Chinese regulators may change our conclusion about the effect of the M&A Rules on us. We cannot, therefore, assure investors that we will not need to potentially obtain in the future the pre-approval from the CSRC or other government agencies prior to conducting a public offering in a foreign capital market.

Furthermore, on July 6, 2021, the General Office of the Central Committee of the Communist Party of China and the General Office of the State Council jointly promulgated the Opinions on Strictly Cracking Down on Illegal Securities Activities in Accordance with the Law, pursuant to which Chinese regulators are required to accelerate rulemaking related to the overseas issuance and listing of securities, and update the existing laws and regulations related to data security, cross-border data flow, and management of confidential information. Numerous regulations, guidelines and other measures have been or are expected to be adopted under the umbrella of or in addition to the Cyber Security Law and Data Security Law. As there are still uncertainties regarding the interpretation and implementation of such regulatory guidance, we cannot assure investors that we will be able to comply with new regulatory requirements relating to our future overseas capital-raising activities, and we may become subject to more stringent requirements with respect to matters including data privacy and cross-border investigation and enforcement of legal claims.

Based on the above and our understanding of the Chinese laws and regulations currently in effect, we were not required to submit an application to the CSRC or Cyberspace Administration of China, or the CAC, for the listing and trading of our ADSs on the Nasdaq. However, there remains significant uncertainty as to the enactment, interpretation and implementation of regulatory requirements related to overseas securities offerings and other capital markets activities. If it is determined in the future that the approval of the CSRC, the CAC or any other regulatory authority is required for offerings of our equity securities, we may face sanctions by the CSRC, the CAC or other Chinese regulatory agencies. These regulatory agencies may impose fines and penalties on our operations in China, limit our ability to pay dividends outside of China, limit our operations in China, delay or restrict the repatriation of the proceeds from our initial public offering into China or take other actions that could have a material adverse effect on our business, financial condition, results of operations and prospects, as well as the trading price of our ADSs and ordinary shares. In addition, if the CSRC, the CAC or other regulatory agencies later promulgate new rules requiring that we obtain their approvals for any future public offerings, we may be unable to obtain a waiver of such approval requirements, if and when procedures are established to obtain such a waiver. Any uncertainties and/or negative publicity regarding such an approval requirement could have a material adverse effect on the trading price of our ADSs and the ordinary shares, including potentially making those ADSs and ordinary shares worthless.

We may face further restrictions (or even prohibitions) on our ability to transfer our scientific data abroad if Chinese regulators impose new restrictions (or change their interpretation of existing restrictions) on life sciences companies like us and the scientific data we obtain, generate, and maintain.

The General Office of the State Council passed the Scientific Data Administrative Measures in March 2018, which provides a regulatory framework for the collection, submission, retention, exploitation, confidentiality and security of scientific data. Scientific data is defined as data generated from basic research, applied research, experiments and developments in the fields of natural sciences, engineering and technology. It also includes the original and derived data by means of surveillance, monitoring, field studies, examination and testing that are used in scientific research activities. All scientific data generated by research entities, including research institutions, higher education institutions and enterprises that is created or managed with government funds, or funded by any source that concerns state secrets, national security, or social and public interests, must be submitted to data centers designated by the Chinese government for consolidation. Disclosure of scientific data will be subject to regulatory scrutiny.

The definition of scientific data is quite broad, but the Chinese government has not issued further guidance to clarify if clinical study data would fall within the definition of scientific data. To our understanding, the Chinese government has not required life sciences companies to upload clinical study data to any government-designated data center, or prevented the cross-border transmission and sharing of clinical study data. None of our clinical study or other scientific data has been created or managed with government funds, or funded by any source that concerns state secrets, national security, or social and public interests. To date, we have received all requisite permissions to transfer clinical study data abroad. We are closely monitoring legal and regulatory developments in this area to see how scientific data is interpreted, and we may be required to comply with additional regulatory requirements for sharing clinical study or other scientific data with our licensors or foreign regulatory authorities, although the scope of such requirements, if any, is currently unknown.

4. *We note your response to prior comment four and updated disclosure on pages 2-3 of your 2021 Q3 Form 10-Q. As requested in the prior comment, please include the disclosures requested in the comment as a separate risk factor as well.*

Response to Comment 4:

The Company acknowledges the Staff's comment and advises the Staff that it will include the disclosures requested in the comment as a separate risk factor in the Company's Form 10-K for the year ending December 31, 2021. Unless there are changes in relevant law or regulations, or in interpretations thereof that would necessitate changes to the below, we will add the following risk factor in response to this comment four:

We may rely on dividends and other distributions on equity paid by our Chinese subsidiaries to fund any cash and financing requirements we may have, and any limitation on the ability of our Chinese subsidiaries to make payments to us could have a material and adverse effect on our ability to conduct our business.

We are a holding company, and we may rely on dividends and other distributions on equity paid by our Chinese subsidiaries for our cash and financing requirements, including the funds necessary to pay dividends and other cash distributions to our shareholders or holders of our ADSs or to service any debt we may incur. If any of our Chinese subsidiaries incur debt on their own behalf in the future, the instruments governing such debt may restrict their ability to pay dividends to us. To date, there have not been any such dividends or other distributions from our Chinese subsidiaries to our subsidiaries located in or outside of China. In addition, as of the date of this Annual Report on Form 10-K, none of our subsidiaries have ever issued any dividends or distributions to us or their respective shareholders in or outside of China, and neither we nor any of our subsidiaries have ever directly or indirectly paid dividends or made distributions to U.S. investors. Zai Lab (Shanghai) Co., Ltd., an operating subsidiary of ours that is domiciled in China, received $266.5 million in capital contributions via twenty-two separate contributions from Zai Lab (Hong Kong) Limited, its sole shareholder, domiciled outside of China, from 2014 to 2021, to fund its business operations in China. Zai Lab International Trading (Shanghai) Co., Ltd., an operating subsidiary of ours that is domiciled in China, received RMB1.0 million in capital contributions via contributions from Zai Lab (Shanghai) Co., Ltd., its sole shareholder, in 2019 to fund its business operations in China. Zai Lab (Suzhou) Co., Ltd., an operating subsidiary of ours that is domiciled in China, received RMB166.5 million in capital contributions via ten separate contributions from Zai Lab (Hong Kong) Limited, its sole shareholder, domiciled outside of China, from 2015 to 2019 to fund its business operations in China. Zai Lab Trading (Suzhou) Co., Ltd., an operating subsidiary of ours that is domiciled in China, received RMB1.0 million in capital contributions via contributions from Zai Lab (Suzhou) Co., Ltd., its sole shareholder, in 2020 to fund its business operations in China. Zai Biopharmaceutical (Suzhou) Co., Ltd., an operating subsidiary of ours that is domiciled in China, received $15.0 million in capital contributions via four separate contributions from Zai Lab (Hong Kong) Limited, its sole shareholder, domiciled outside of China, from 2017 to 2018 to fund its business operations in China. In the future, cash proceeds raised from our overseas financing activities may be transferred by us to our Chinese subsidiaries via capital contribution or shareholder loans or intercompany loans, as the case may be.

According to the Foreign Investment Law of the People's Republic of China and its implementing rules, which jointly established the legal framework for the administration of foreign-invested companies, a foreign investor may, in accordance with other applicable laws, freely transfer into or out of China its contributions, profits, capital earnings, income from asset disposal, intellectual property rights, royalties acquired, compensation or indemnity legally obtained, and income from liquidation, made or derived within the territory of China in RMB or any foreign currency, and any entity or individual shall not illegally restrict such transfer in terms of the currency, amount and frequency. According to the Company Law of the People's Republic of China and other Chinese laws and regulations, our Chinese subsidiaries may pay dividends only out of their respective accumulated profits as determined in accordance with Chinese accounting standards and regulations. In addition, each of our Chinese subsidiaries is required to set aside at least 10% of its accumulated after-tax profits, if any, each year to fund a certain statutory reserve fund, until the aggregate amount of such fund reaches 50% of its registered capital. Where the statutory reserve fund is insufficient to cover any loss the Chinese subsidiary incurred in the previous financial year, its current financial year's accumulated after-tax profits shall first be used to cover the loss before any statutory reserve fund is drawn therefrom. Such statutory reserve funds and the accumulated after-tax profits that are used for covering the loss cannot be distributed to us as dividends. At their discretion, our Chinese subsidiaries may allocate a portion of their after-tax profits based on Chinese accounting standards to a discretionary reserve fund.

RMB is not freely convertible into other currencies. As a result, any restriction on currency exchange may limit the ability of our Chinese subsidiaries to use their potential future RMB revenues to pay dividends to us. The Chinese government imposes controls on the convertibility of RMB into foreign currencies and, in certain cases, the remittance of currency out of China. Shortages in availability of foreign currency may then restrict the ability of our Chinese subsidiaries to remit sufficient foreign currency to our offshore entities for our offshore entities to pay dividends or make other payments or otherwise to satisfy our foreign-currency-denominated obligations. RMB is currently convertible under the "current account," which includes dividends, trade and service-related foreign exchange transactions, but not under the "capital account," which includes foreign direct investment and foreign debt (which may be denominated in foreign currency or RMB), including loans we may secure for our Chinese subsidiaries. Currently, our Chinese subsidiaries may purchase foreign currency for settlement of current account transactions, including payment of dividends to us, without the approval of the State Administration of Foreign Exchange of China (SAFE) by complying with certain procedural requirements. However, the relevant Chinese governmental authorities may limit or eliminate our ability to purchase foreign currencies in the future for current account transactions. The Chinese government may continue to strengthen its capital controls, and additional restrictions and substantial vetting processes may be instituted by SAFE for cross-border transactions falling under both the current account and the capital account. Any existing and future restrictions on currency exchange may limit our ability to utilize revenue generated in RMB to fund our business activities outside of China or pay dividends in foreign currencies to holders of our securities. Foreign exchange transactions under the capital account remain subject to limitations and require approvals from, or registration with, SAFE and other relevant Chinese governmental authorities. This could affect our ability to obtain foreign currency through debt or equity financing for our subsidiaries.

5. *We note your response to prior comment seven. As requested in the prior comment, please expand the disclosures in your risk factors. For example, on page 49 of your 2021 Q3 Form 10-Q, expand your disclosures to state that the Chinese government may intervene or influence your operations at any time, which could result in a material change in your operations and/or the value of your ADSs and any action by the Chinese government to exert more oversight and control over offerings that are conducted overseas and/or foreign investment in China-based issuers could significantly limit or completely hinder your ability to offer or continue to offer securities to investors and cause the value of such securities to significantly decline or be worthless.*

Response to Comment 5:

The Company acknowledges the Staff's comment and advises the Staff that it will expand its disclosures in its risk factors in the Company's Form 10-K for the year ending December 31, 2021. Unless there are changes in relevant law or regulations, or in interpretations thereof that would necessitate changes to the below, we will add the following risk factor in response to this comment five:

The Chinese government may intervene in or influence our operations at any time, which could result in a material change in our operations and significantly and adversely impact the value of our ADSs, including potentially making those ADSs worthless.

The Chinese government has significant oversight and discretion over the conduct of our business and may intervene or influence our operations as the government deems appropriate to further regulatory, political and societal goals. The Chinese government has recently published new policies that significantly affected certain industries such as the education and internet industries, and we cannot rule out the possibility that it will in the future release regulations or policies regarding the life sciences industry that could require us to seek permission from Chinese authorities to continue to operate our business, which may adversely affect our business, financial condition and results of operations. Furthermore, recent statements made by the Chinese government have indicated an intent to increase the government's oversight and control over offerings of companies with significant operations in China that are to be conducted in foreign markets, as well as foreign investment in China-based issuers like us. Any such action taken by the Chinese government could significantly limit or completely hinder our ability to offer or continue to offer ADSs to our investors and could cause the value of our ADSs to significantly decline or become worthless.

6. *We note your response to prior comment eight and updated disclosure on page 45 of your 2021 Q3 Form 10-Q. As requested in the prior comment, please expand your risk factor disclosure to explain to what extent you believe that you are compliant with the regulations or policies that have been issued by the CAC to date.*

Response to Comment 6:

The Company acknowledges the Staff's comment and advises the Staff that it will expand its risk factor disclosure in the Company's Form 10-K for the year ending December 31, 2021. Unless there are changes in relevant law or regulations, or in interpretations thereof that would necessitate changes to the below, we will add the following risk factor in response to this comment six:

Compliance with China's Data Security Law, Cyber Security Law, Cybersecurity Review Measures, Personal Information Protection Law, the Regulation on the Administration of Human Genetic Resources, the Biosecurity Law and any other future laws and regulations may entail significant expenses and could materially affect our business. Our failure to comply with such laws and regulations could lead to government enforcement actions and significant penalties against us, materially and adversely impacting our operating results.

China has implemented extensive data protection, privacy, and information security rules and is considering a number of additional proposals relating to these subject areas. Based on our understanding of these laws, regulations, and policies—some of which were only recently-enacted—and the government regulators' interpretation of those legal requirements as applied to life sciences companies like us, we believe we are compliant with all of our material legal obligations. Nevertheless, we face significant uncertainties and risks which, as explained below, may materially and adversely affect our operations.

We maintain personally identifiable health information of patients in China in limited situations. We also collect and maintain de-identified or anonymized health data for clinical trials in compliance with local regulations. This data could be deemed by government regulators to be "personal data" or "important data." With China's growing emphasis on its sovereignty over data derived from China, the outbound transmission of de-identified or anonymized health data for clinical trials may be subject to the new national security legal regime, including the Data Security Law, the Cyber Security Law of the People's Republic of China, or the Cyber Security Law, the Personal Information Protection Law, or the PIPL, the Regulation on the Administration of Human Genetic Resource, and various implementing regulations and standards.

China's Data Security Law took effect in September 2021. The Data Security Law provides that the data processing activities must be conducted based on "data classification and hierarchical protection system" for the purpose of data protection and prohibits entities in China from transferring data stored in China to foreign law enforcement agencies or judicial authorities without prior approval by the Chinese government. The classification of data is based on its importance in economic and social development, as well as the degree of harm expected to be caused to national security, public interests, or the legitimate rights and interests of individuals or organizations if such data is tampered with, destroyed, leaked, or illegally acquired or used. The security assessment mechanism was also included in the PIPL, which was promulgated in August 2021 and became effective on November 1, 2021, for the Chinese government to supervise certain cross-border transfers of personal information.

Additionally, the Cyber Security Law, which became effective in 2017, requires companies to take certain organizational, technical and administrative measures and other necessary measures to ensure the security of their networks and data stored on their networks. Specifically, the Cyber Security Law provides that companies adopt a multi-level protection scheme, or MLPS, under which network operators are required to perform obligations of security protection to ensure that the network is free from interference, disruption or unauthorized access, and prevent network data from being disclosed, stolen or tampered. Under the MLPS, entities' operating information systems must have a thorough assessment of the risks and the conditions of their information and network systems to determine the level to which the entity's information and network systems belong – from the lowest Level 1 to the highest Level 5 pursuant to a series of national standards on the grading and implementation of the classified protection of cyber security. The grading result will determine the set of security protection obligations that entities must comply with. Entities classified as Level 2 or above should report the grade to the relevant government authority for examination and approval.

Under the Cyber Security Law and Data Security Law, we are required to establish and maintain a comprehensive data and network security management system that will enable us to monitor and respond appropriately to data security and network security risks. We will need to classify and take appropriate measures to address risks created by our data processing activities and use of networks. We are obligated to notify affected individuals and appropriate Chinese regulators of and respond to any data security and network security incidents. Establishing and maintaining such systems takes substantial time, effort and cost, and we may not be able to establish and maintain such systems as fully as needed to ensure compliance with our legal obligations. Despite our investment, such systems may not adequately protect us or enable us to appropriately respond to or mitigate all data security and network security risks or incidents we face.

Furthermore, under the Data Security Law, data categorized as "important data," which will be determined by governmental authorities in the form of catalogs, is to be processed and handled with a higher level of protection. The notion of important data is not clearly defined by the Cyber Security Law or the Data Security Law. In order to comply with the statutory requirements, we will need to determine whether we possess important data, monitor the important data catalogs that are expected to be published by local governments and departments, perform risk assessments and ensure we are complying with reporting obligations to applicable regulators. We may also be required to disclose to regulators business-sensitive or network security-sensitive details regarding our processing of important data, and may need to pass the government security review or obtain government approval in order to share important data with offshore recipients, which can include foreign licensors, or share data stored in China with judicial and law enforcement authorities outside of China. If judicial and law enforcement authorities outside China require us to provide data stored in China, and we are not able to pass any required government security review or obtain any required government approval to do so, we may not be able to meet the foreign authorities' requirements. The potential conflicts in legal obligations could have adverse impact on our operations in and outside of China.

Recently, the CAC has taken action against several Chinese internet companies listed on U.S. securities exchanges for alleged national security risks and improper collection and use of the personal information of Chinese data subjects. According to the official announcement, the action was initiated based on the National Security Law, the Cyber Security Law and the Measures on Cybersecurity Review, which are aimed at "preventing national data security risks, maintaining national security and safeguarding public interests." On December 28, 2021, the CAC published the Cybersecurity Review Measures, which will be effective on February 15, 2022, expanding the cybersecurity review to data processing operators in possession of personal information of over 1 million users if the operators intend to list their securities in a foreign country. We do not currently possess personal information of more than 1 million users.

On October 29, 2021, the CAC published the Measures on Security Assessment of Outbound Data Transfers (Draft for Comment), or the Draft Measures. The Draft Measures are enacted in accordance with the Cyber Security Law, the Data Security Law and the PIPL. Under the Draft Measures, a data processor would be subject to mandatory security assessment for transfers of data out of China under any of the following circumstances: (i) where the outbound data is personal information and important data collected and generated by critical information infrastructure operators; (ii) where the outbound data contains important data; (iii) where a personal information processor that has processed personal information of more than one million people transfers personal information overseas; (iv) where the personal information of more than 100,000 people or sensitive personal information of more than 10,000 people is transferred overseas accumulatively; or (v) other circumstances under which a security assessment of outbound data transfers is required as prescribed by the CAC. It is unclear at the present time how widespread the cybersecurity review requirement and the enforcement action will be and what effect they will have on the life sciences sector generally and the Company in particular. China's regulators may impose penalties for non-compliance ranging from fines or suspension of operations, and this could lead to us delisting from the U.S. stock market. Currently, we have not been involved in any investigations on cybersecurity review initiated by the CAC or related governmental regulatory authorities, and we have not received any inquiry, notice, warning, or sanction in such respect.

The National People's Congress released the PIPL, which became effective on November 1, 2021. The PIPL provides a comprehensive set of data privacy and protection requirements that apply to the processing of personal information and expands data protection compliance obligations to cover the processing of personal information of persons by organizations and individuals in China, and the processing of personal information of persons in China outside of China if such processing is for purposes of providing products and services to, or analyzing and evaluating the behavior of persons in China. The PIPL also provides that "critical information infrastructure operators" and "personal information processing entities" who process personal information meeting a volume threshold to be set by Chinese cyberspace regulators are also required to store in China personal information generated or collected in China, and to pass a security assessment administered by Chinese cyberspace regulators for any export of such personal information. Lastly, the PIPL contains proposals for significant fines for serious violations of up to RMB 50 million or 5% of annual revenues from the prior year and violators may also be ordered to suspend any related activity by competent authorities. We do not believe that, based on our understanding of the PIPL and its interpretation by the authorities, that we are either a critical information infrastructure operator or process a sufficient amount of personal information to be a personal information processing entity subject to the above storage and security assessment requirements.

In addition, certain industry-specific laws and regulations affect the collection and transfer of personal data in China. For example, the Regulation on the Administration of Human Genetic Resources, or the HGR Regulation, promulgated by the State Council of the People's Republic of China, or the State Council, which became effective on July 1, 2019, applies to activities that involve collection, biobanking, use of human genetic resources (HGR), which includes the genetic materials with respect to organs, tissues, cells and other materials that contain the human genome, genes and other genetic substances (the China Biospecimens) and derived data in China (together with the China Biospecimens, the China-Sourced HGR), and the provision of such items to foreign parties or entities established or actually controlled by them. The HGR Regulation prohibits both onshore and offshore entities established or actually controlled by foreign entities and individuals from collecting or biobanking any China-Sourced HGR in China, as well as providing such China-Sourced HGR outside of China. Chinese parties are required to seek an advance approval for the collection and biobanking of all China-Sourced HGR. Approval for any export or cross-border transfer of China-Sourced HGR in the form of biospecimens is required, and transfer of derived data by Chinese parties to foreign parties or entities established or actually controlled by them also requires the Chinese parties to file, before the transfer, a copy of the data with the Human Genetic Resources Administration of China, or HGRAC, for record purposes and to obtain a notification filing number in order to transfer the data. The HGR Regulation also requires that foreign parties or entities established or actually controlled by them ensure the full participation of Chinese parties in international collaborations and share all records and data with the Chinese parties.

To further tighten the control of China-Sourced HGR, the Standing Committee of the National People's Congress of the People's Republic of China, or the SCNPC, issued the Eleventh Amendment to the Criminal Law of the People's Republic of China on December 26, 2020, which became effective on March 1, 2021, criminalizing the illegal collection of China-Sourced HGR and the illegal transfer of China-sourced biospecimens outside of China, and the transfer of China-sourced derived data to foreign parties or entities established or actually controlled by them without going through security review and assessment. An individual who is convicted of any of these violations may be subject to public surveillance, criminal detention, a fixed-term imprisonment of up to seven years and/or a criminal fine. In October 2020, the SCNPC adopted the Biosecurity Law of the People's Republic of China, or the Biosecurity Law, which became effective on April 15, 2021. The Biosecurity Law will establish an integrated system to regulate biosecurity-related activities in China, including, among others, the security regulation of HGR and biological resources. The Biosecurity Law for the first time expressly declared that China has sovereignty over its HGR, and further endorsed the HGR Regulation by recognizing the fundamental regulatory principles and systems established by it over the utilization of China-Sourced HGR by foreign parties or entities established or actually controlled by them in China. Though the Biosecurity Law does not provide any specific new regulatory requirements on HGR, as it is a law adopted by China's highest legislative authority, it gives China's primary regulator of HGR, the Ministry of Science and Technology, or MOST, significantly more power and discretion to regulate HGR and it is expected that the overall regulatory landscape for China-Sourced HGR will evolve and become even more rigorous and sophisticated. In addition, the interpretation and application of data protection laws in China and elsewhere are often uncertain and in flux.

So far, the HGRAC has disclosed a number of HGR violation cases. In one case, the sanctioned party was the Chinese subsidiary of a multinational pharmaceutical company that was found to have illegally transferred certain biospecimens to CROs for conducting certain unapproved research. In addition to a written warning and confiscation of relevant HGR materials, the Chinese subsidiary of the multinational pharmaceutical company was requested by the HGRAC to take rectification measures and was also banned by the HGRAC from submitting any clinical trial applications until the HGRAC was satisfied with the rectification results, which rendered it unable to initiate new clinical trials in China until the ban was lifted. In another case, the CRO engaged by the Chinese subsidiary of a multinational pharmaceutical company was found to have forged an ethics committee approval in order to accelerate the HGRAC approval. Both the Chinese subsidiary of the multi-national pharmaceutical company and the CRO were debarred from initiating new applications for a period of 6 to 12 months, respectively.

Interpretation, application and enforcement of these laws, rules and regulations evolve from time to time and their scope may continually change, through new legislation, amendments to existing legislation or changes in enforcement. Compliance with the Cyber Security Law, the Data Security Law and other related laws and regulations could significantly increase the cost to us of providing our products, require significant changes to our operations or even prevent us from providing certain products in jurisdictions in which we currently operate or in which we may operate in the future. Despite our efforts to comply with applicable laws, regulations and other obligations relating to privacy, data protection and information security, it is possible that our practices, products or platform could fail to meet all of the requirements imposed on us by the Cyber Security Law, the Data Security Law and/or related implementing regulations. Any failure on our part to comply with such law or regulations or any other obligations relating to privacy, data protection or information security, or any compromise of security that results in unauthorized access, use or release of personally identifiable information or other data, or the perception or allegation that any of the foregoing types of failure or compromise has occurred, could damage our reputation, discourage new and existing counterparties from contracting with us or result in investigations, fines, suspension or other penalties by Chinese government authorities and private claims or litigation, any of which could materially adversely affect our business, financial condition and results of operations. If the Chinese parties fail to comply with data privacy and cybersecurity laws, regulations and practice standards, and our research data is obtained by unauthorized persons, used or disclosed inappropriately or destroyed, we may lose our confidential information and be subject to litigation and government enforcement actions. It is possible that these laws may be interpreted and applied in a manner that is inconsistent with our or our collaborators' practices, potentially resulting in suspension of relevant ongoing clinical trials or delays in the initiation of new trials, confiscation of China-Sourced HGR, administrative fines, disgorgement of illegal gains or temporary or permanent debarment of our or our collaborators' entities and responsible persons from further clinical trials and, consequently, a de-facto ban on the debarred entities from initiating new clinical trials in China. In addition, a data breach affecting personal information, including health information, or a failure to comply with applicable requirements could result in significant management resources, legal and financial exposure and reputational damage that could potentially have a material adverse effect on our business and results of operations. Even if our practices are not subject to legal challenge, the perception of privacy concerns, whether or not valid, may harm our reputation and brand and adversely affect our business, financial condition and results of operations. Moreover, the legal uncertainty created by the Data Security Law and Cybersecurity Review Measures and the recent Chinese government actions could materially adversely affect our ability, on favorable terms, to raise capital in the U.S. market in the future.

The national security legal regime imposes stricter data localization requirements on personal information and human health-related data and may require us to undergo cybersecurity or other security review, obtain government approval or certification, or put in place certain contractual protections before transferring personal information and human health-related data out of China. As a result, personal information, important data and health and medical data that we or our customers, vendors, clinical trial sites, pharmaceutical partners and other third parties collect, generate or process in China may be subject to such data localization requirements and heightened regulatory oversight and controls. We may need to maintain local data centers in China, conduct security assessments or obtain the requisite approvals from the Chinese government for the transmission outside of China of such controlled information and data, which could significantly increase our operating costs or cause delays or disruptions in our business operations in and outside China. We expect that the evolving regulatory interpretation and enforcement of the national security legal regime will lead to increased operational and compliance costs and will require us to continually monitor and, where necessary, make changes to our operations, policies, and procedures. If our operations, or the operations of our CROs, licensees or partners, are found to be in violation of these requirements, we may suffer loss of use of data, suffer a delay in obtaining regulatory approval for our products, be unable to transfer data out of China, be unable to comply with our contractual requirements, suffer reputational harm or be subject to penalties, including administrative, civil and criminal penalties, damages, fines and the curtailment or restructuring of our operations. If any of these were to occur, it could materially adversely affect our ability to operate our business and our financial results.

7. *Please revise both the risk factors summary and the Risk Factors section to move forward the risks related to doing business in the PRC so that such risks are prominently disclosed within each section in relation to other identified material risks.*

Response to Comment 7:

The Company acknowledges the Staff's comment and advises the Staff that it will revise both the Risk Factors Summary and the Risk Factors sections to move forward the risks related to doing business in the PRC in the Company's Form 10-K for the year ending December 31, 2021 so that risks are prominently disclosed with each section in relation to other identified material risks.

* * *

We hope that the foregoing has been responsive to the Staff's comments. If you have any questions about this letter or require any further information, please call my office at (617) 235-4961.

Very truly yours,

/s/ Thomas J. Danielski
Thomas J. Danielski

cc: F. Ty Edmondson
Billy Cho