February 21, 2023

VIA EDGAR & E-MAIL

Securities and Exchange Commission
Division of Corporation Finance
Office of Trade & Services
100 F Street, N.E.
Washington, D.C. 20549
Attn: Taylor Beech
Mara Ransom

Re: Yum China Holdings, Inc.
Form 10-K for the Year Ended December 31, 2021
Correspondence Filed January 3, 2023
File No. 1-37762

Ladies and Gentlemen:

Yum China Holdings, Inc. (the "Company") is pleased to respond to the letter dated February 2, 2023 from the staff (the "Staff") of the Securities and Exchange Commission with respect to the Company's annual report on Form 10-K for the year ended December 31, 2021. For the convenience of the Staff's review, we have set forth below the comment contained in the Staff's letter in italics followed by the Company's response.

Correspondence Filed January 3, 2023

Item 1A. Risk Factors, page 9

1. *We note your response to comment 10. Revise to state whether you believe that you are compliant with the regulations or policies that have been issued by the CAC to date, notwithstanding the various uncertainties you disclose. In this regard, we are not aware of any regulatory process in which you are expected to be identified as a "critical information infrastructure operator" before ensuring compliance with the Revised Cybersecurity Review Measures.*

Company Response:

In future annual reports, the Company proposes to make the following revisions to the below risk factor (with revisions in response to the Staff's additional comment in bold):

Unauthorized access to, or improper use, disclosure, theft or destruction of, our customer or employee personal, financial or other data or our proprietary or confidential information that is stored in our information systems or by third parties on our behalf could result in substantial costs, expose us to litigation and damage our reputation.

We have been using, and plan to continue to use, digital technologies to improve the customer experience and drive sales growth. We, directly or indirectly, receive and maintain certain personal, financial and other information about our customers in various information systems that we maintain and in those maintained by third-party service providers when, for example, receiving orders through mobile or online platforms, accepting digital payments, operating loyalty programs and conducting digital marketing programs. Our information technology systems, such as those we use for administrative functions, including human resources, payroll, accounting and internal and external communications, can contain personal, financial or other information of our over 450,000 employees. We also maintain important proprietary and other confidential information related to our operations and identifiable information about our franchisees. As a result, we face risks inherent in handling and protecting large volumes of information.

If our security and information systems or the security and information systems of third-party service providers are compromised for any reason, including as a result of data corruption or loss, security breach, cyber-attack or other external or internal methods, or if our employees, franchisees or service providers fail to comply with laws, regulations and practice standards, and this information is obtained by unauthorized persons, used or disclosed inappropriately or destroyed, it could subject us to litigation and government enforcement actions, cause us to incur substantial costs, liabilities and penalties and/or result in a loss of customer confidence, any and all of which could adversely affect our business, reputation, ability to attract new customers, results of operations and financial condition.

In addition, the use and handling of this information is regulated by evolving and increasingly demanding laws and regulations. The Chinese government has focused increasingly on regulation in the areas of information security and protection, including by implementing the PRC Cybersecurity Law effective June 1, 2017, which imposes tightened requirements on data privacy and cybersecurity practices. There are uncertainties with respect to the application of the cybersecurity law in certain circumstances. In addition, the PRC Data Security Law, which took effect on September 1, 2021, imposes data security and privacy obligations on entities and individuals carrying out data activities (including activities outside of the PRC), requires a national security review of data activities that may affect national security, and imposes restrictions on data transmissions. Furthermore, the PRC Personal Information Protection Law, which took effect on November 1, 2021, sets out the regulatory framework for handling and protection of personal information and transmission of personal information, and many specific requirements of the law remain to be clarified by the Cyberspace Administration of China (the "CAC") and other regulatory authorities. The Revised Cybersecurity Review Measures, which took effect on February 15, 2022, require critical information infrastructure operators procuring network products and services and online platform operators carrying out data processing activities, which

affect or may affect national security, to conduct a cybersecurity review pursuant to the provisions therein. The Measures for Security Assessment for Outbound Data Transfer, which took effect on September 1, 2022, mandate mandatory government security review by the CAC in advance of certain cross-border data transfer activities. **We have established a professional team to formulate and implement internal data security policies to comply with the regulations and policies issued by the CAC, monitor our compliance practices and assess any non-compliance issues. We believe that we are compliant in all material respects with the applicable regulations and policies that have been issued by the CAC to date. As of the date of this annual report, (i)** ~~no detailed rules or implementation rules of the Measures for Cybersecurity Review have been issued by any PRC authority;~~ **we have not received any formal notice from any PRC cybersecurity regulator identifying us as a "critical information infrastructure operator" or requiring us to go through the cybersecurity review procedures pursuant to the Revised Cybersecurity Review Measures; and (ii) we are not aware of any investigations against us initiated by the CAC based on the Revised Cybersecurity Review Measures.** ~~Furthermore, t~~The exact scope of "critical information infrastructure operators" under the current regulatory regime remains unclear, and the PRC government authorities may have wide discretion in the interpretation and enforcement of the applicable laws. Therefore, it is uncertain whether, in the future, we would be deemed to be a critical information infrastructure operator under PRC law. If we are deemed to be a critical information infrastructure operator under the PRC cybersecurity laws and regulations, we may be subject to obligations in addition to what we have fulfilled under the PRC cybersecurity laws and regulations.

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. We have been taking and will continue to take reasonable measures to comply with applicable cybersecurity, data privacy and security laws. We cannot guarantee the effectiveness of the measures undertaken by us, and such measures may still be determined as insufficient, improper, or even as user-privacy invasive, by the relevant authorities, which may result in penalties against us.

Compliance with these laws, as well as additional regulations and standards regarding data privacy, data collection and information security that PRC regulatory bodies may enact in the future, may result in additional expenses to us as we may be required to upgrade our current information technology systems. Furthermore, as a result of legislative and regulatory rules, we may be required to notify the owners of information of any breach, theft or loss of their information, which could harm our reputation, as well as subject us to litigation or actions by regulatory bodies and adversely affect our financial results.

We expect that cybersecurity, data privacy and security will continue to be a focus of regulators, as well as attract continued or greater public scrutiny and attention going forward, which could increase our compliance costs and subject us to heightened risks and challenges associated with information security and protection. If we are unable to manage these risks, we could become subject to penalties, including fines, suspension of

business, shutdown of websites and revocation of required licenses, and our reputation and results of operations could be materially and adversely affected.

~~As of the date of this annual report, we believe, to the best of our knowledge, our business operations do not violate any of the above laws and regulations currently in force in any material respect, including those that have been issued by CAC, as of the date of this annual report.~~

*****

Thank you for your consideration in reviewing the above response. We note that all proposed future disclosures remain subject to further revision in response to business and regulatory developments that may affect the Company between now and the filing of its next annual report. Please contact me at Joseph.Chan@YumChina.com with any questions.

Sincerely,

/s/ Joseph Chan

Joseph Chan
Chief Legal Officer