

Antony Kim
Direct Dial: +1.202.637.3394
antony.kim@lw.com

555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Tel: +1.202.637.2200 Fax: +1.202.637.2201
www.lw.com

LATHAM & WATKINS LLP

FIRM / AFFILIATE OFFICES

| | |
|--------------|------------------|
| Austin | Milan |
| Beijing | Munich |
| Boston | New York |
| Brussels | Orange County |
| Century City | Paris |
| Chicago | Riyadh |
| Dubai | San Diego |
| Düsseldorf | San Francisco |
| Frankfurt | Seoul |
| Hamburg | Shanghai |
| Hong Kong | Silicon Valley |
| Houston | Singapore |
| London | Tel Aviv |
| Los Angeles | Tokyo |
| Madrid | Washington, D.C. |

April 13, 2023

VIA EMAIL

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
consumer@ag.iowa.gov

Re: **Notice of Data Security Incident Relating to Iowa Residents**

Dear Sir/Madam:

On or around January 13, 2023, Yum! Brands, Inc. experienced a ransomware attack that resulted in unauthorized access to certain of its systems. Upon discovery, Yum! took steps to lock down impacted systems, notified and cooperated with federal law enforcement authorities, and engaged digital forensic experts to determine what happened and what information was exposed. On January 18, 2023, Yum! publicly disclosed the incident through a Form 8-K filing¹.

On March 9, 2023, Yum! determined that the impacted systems contained personal information of approximately 513 Iowa residents, who are current or former Yum! employees or their dependents. While the specific data elements vary by individual, the exposed personal information generally includes Social Security Numbers, government identification numbers, date of birth, health insurance information, and medical information. Notification letters are being sent to residents by mail starting on April 14th, 2023, together with an offer for two years of complimentary credit monitoring and identity theft protection services provided by IDX (see Appendix A).

As part of its ongoing operations and in response to this incident, Yum! has deployed advanced security tooling across its network and engaged in tactical security hardening activities,

¹ See <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001041061/d9c666b5-7be0-40a5-8322-52644767bd76.pdf>

LATHAM & WATKINSLLP

as well as dark web monitoring. Yum! is also reviewing its security policies and procedures and identifying opportunities for enhancement.

If your office requires any further information in regards to this matter, please contact me at (202) 637-3394 or tony.kim@lw.com.

Respectfully submitted,

A handwritten signature in black ink that reads "Antony P. Kim". The signature is written in a cursive, flowing style.

Antony Kim
of LATHAM & WATKINS LLP

Enclosure

Appendix A



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
888-566-0758
Or Visit:
<https://response.idx.us/YumRSG>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

April 14, 2023

Re: Notice of Security Breach

Dear <<First Name>> <<Last Name>>:

We are writing to provide you with information about a cybersecurity incident involving your personal information that occurred in mid-January 2023. While we have no evidence of identity theft or fraud involving your data, we wanted to share some details and offer you some resources that you may find helpful. Please note the section titled "What You Can Do" below.

What Happened? As we announced publicly in mid-January, Yum! experienced a cybersecurity incident involving unauthorized access to certain of our systems on or around January 13, 2023. Upon discovery, we took steps to lock down impacted systems, notified federal law enforcement authorities, worked with leading digital forensics and restoration teams to investigate and recover from the incident, and deployed enhanced 24/7 detection and monitoring technology. Once the incident was contained, we initiated a detailed review, with the assistance of outside specialists, to identify whether personal information belonging to individuals may have been present in files that were affected during the incident.

What Information is Involved? Our review determined that the exposed files contained some of your personal information, including <<Personal Information Impacted>>.

What Are We Doing? As noted above, we have no evidence of identity theft or fraud involving your personal information, but we are contacting you out of an abundance of caution to offer support and provide resources.

What You Can Do. As a matter of general precaution, it is always good practice to be vigilant against identity theft and fraud by reviewing your account statements and monitoring any available credit reports for unauthorized or suspicious activity, and by taking care in response to any email, telephone or other contacts that ask for personal or sensitive information (e.g., phishing). Yum! will never request sensitive information by phone or email. You may also review the attached *Steps You Can Take to Help Protect Your Information* as a helpful resource.

We are also providing complimentary credit monitoring and identity protection services for 2 years via IDX. These services include credit monitoring, a \$1,000,000 insurance reimbursement policy and full managed identity restoration in the event that you fall victim to identity theft, and dark web monitoring to monitor if your data appears in illicit online forums. To activate these services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Your Information*.



For More Information. For further information, please call 888-566-0758 Monday to Friday 9 am – 9 pm Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Scott Catlett". The signature is stylized with a long horizontal line extending from the end of the name.

Scott Catlett
Chief Legal & Franchise Officer, Corporate Secretary
Yum! Brands, Inc.

Steps You Can Take to Help Protect Your Information

Enroll in IDX Credit Monitoring and Identity Protection Services

Go to <https://response.idx.us/YumRSG> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is July 14, 2023.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file with the credit reporting bureau. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

If you discover any suspicious items on your credit reports or from the fraud alert and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, free of charge, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency filed by you concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

| Equifax | Experian | TransUnion |
|---|---|---|
| https://www.equifax.com/personal/credit-report-services/ | https://www.experian.com/help/ | https://www.transunion.com/credit-help |
| 888-298-0045 | 1-888-397-3742 | 833-395-6938 |
| Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 | Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 | TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016 |
| Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788 | Experian Credit Freeze P.O. Box 9554 Allen, TX 75013 | TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094 |

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud (this letter alone does not suggest that you are a victim of or at risk of identity theft or fraud). Please note that in order for you to file a police report for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California residents, the California Office of Privacy Protection (www.oag.ca.gov/privacy) may be contacted for additional information on protection against identity theft. The California Attorney General can be contacted at 1300 I Street, Sacramento, CA 95814, www.oag.ca.gov, 800-952-5225.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 888-743-0023.

For North Carolina residents, the North Carolina Attorney General can be contacted at Mail Service Center 9001, Raleigh, NC 27699, www.ncdoj.gov, 877-566-7226.

For Rhode Island residents, the Rhode Island Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400. You have the right to file or obtain a police report regarding this incident.

For District of Columbia residents, the District of Columbia Attorney General can be contacted at 400 6th Street NW, Washington, DC 20001, www.oag.dc.gov, 202-727-3400.

For Iowa residents, the Iowa Attorney General can be contacted at 1305 E. Walnut Street, Des Moines, Iowa 50319, www.ag.iowa.gov, 515-281-5926 or 888-777-4590.

For New York residents, the New York Attorney General may be contacted at the Capital, Albany, NY 12224, www.ag.ny.gov, 800-771-7755.

For Oregon residents, the Oregon Attorney General may be reached at 1162 Court Street NE, Salem, OR 97301, www.dog.state.or.us, 503-378-6002.

For South Carolina residents, the South Carolina Department of Consumer Affairs may be reached at 293 Greystone Blvd., Ste. 400, Columbia, SC 29210, www.consumer.sc.gov, 800-922-1594.

For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capital Avenue, Suite 118, Frankfort, KY 40601, www.ag.ky.gov, 502-696-5300.

For Massachusetts residents, you have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, you have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.