FOLEY
FOLEY & LARDNER LLP

ATTORNEYS AT LAW
777 EAST WISCONSIN AVENUE
MILWAUKEE, WI 53202-5306
414.271.2400 TEL
414.297.4900 FAX
WWW.FOLEY.COM

jurban@foley.com
414.297.5864

CLIENT/MATTER NUMBER
046151-2031

April 15, 2021

VIA CERTIFIED MAIL

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Office of the Attorney General:

We are writing on behalf of our client, Kohler Hospitality, which manages Destination Kohler ("KH"), to notify you of a breach of security involving three (3) New Hampshire residents. For background, Destination Kohler is a resort in Kohler, Wisconsin with multiple lodging locations, including The American Club. According to the information provided to KH by its third-party booking solutions provider, TravelClick, the only lodging location at Destination Kohler where New Hampshire residents booked overnight stays that was potentially impacted was The American Club.

NATURE OF THE UNAUTHORIZED DISCLOSURE

On January 21, 2021, one of KH's employees was the victim of a sophisticated phishing attack that compromised their account credentials to KH's third-party reservations system managed by TravelClick after inadvertently responding to a malicious email that appeared to contain a legitimate link to TravelClick's web portal.

As soon as the employee reported the phishing attack to KH on January 21, 2021, KH immediately notified TravelClick and prevented other users from accessing the phishing email. KH also requested that TravelClick immediately cancel the employee's account and create a new account for that user.

On March 11, 2021, KH was informed by TravelClick that it had been conducting a confidential investigation into a potential security incident and determined that the KH employee's credentials may have been used by an unauthorized third party to log in to KH's third-party reservations system managed by TravelClick and potentially access certain payment card information associated with KH guests' reservations booked with The American Club with overnight stay dates between November 29, 2020 and December 1, 2021. According to the information provided to KH by TravelClick, this payment card information included cardholder name, card number, and expiration date. However, TravelClick has stated that cardholders' PINs and security codes were not available or impacted.

Up until KH received notice from TravelClick on March 11, 2021, KH had no reason to believe that any of its guests' personal information was at risk, nor did KH know that TravelClick was conducting an investigation into a potential security incident. Although KH has no evidence to suggest that any of its guests' payment card information was actually accessed or misused by an unauthorized third party, it notified individuals out of an abundance of caution.

STEPS WE ARE TAKING RELATED TO THE INCIDENT

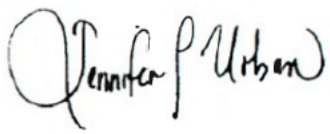
KH mailed a notification to the potentially affected New Hampshire residents on April 15, 2021 pursuant to N.H. Rev. Stat. § 359-C:20. Enclosed is a sample copy of the notice that was sent to those individuals.

As a precautionary measure, KH has provided the potentially affected New Hampshire residents with credit monitoring and identity protection services through TransUnion Interactive, a subsidiary of TransUnion®, at no charge for a period of twenty-four (24) months, and has also set up a dedicated support line that will be staffed to answer any questions individuals may have about this incident or the services available to them.

In response to this incident, KH is reviewing its contracts with third-party vendors for hospitality bookings and reevaluating their privacy and security controls to determine whether any updates are necessary.

If you have any further inquiries concerning this notification, please do not hesitate to contact me.

Sincerely,



Jennifer L. Urban
Foley & Lardner LLP

Encl: Sample Notification Letter

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>> :

You are a valued customer of The American Club, and the privacy and protection of your information is a matter we take very seriously. As a precautionary matter, we are writing to inform you of a recent security incident that may involve some of the information you provided in connection with your reservation(s) booked with our property that was stored by our third-party booking solutions provider, TravelClick.

WHAT HAPPENED?

On January 21, 2021, one of our employees was the victim of a sophisticated phishing attack that compromised their TravelClick login credentials after inadvertently responding to a malicious email that appeared to contain a legitimate link to TravelClick's web portal.

WHAT INFORMATION WAS INVOLVED?

On March 11, 2021, we were informed by TravelClick that it had been conducting a confidential investigation into a potential security incident and determined that our employee's credentials may have been used by an unauthorized third party to log in to our third-party reservations system managed by TravelClick and potentially access certain payment card information associated with our guests' reservations, including cardholder name, card number, and expiration date. However, TravelClick has stated that cardholders' PINs and security codes were not available or impacted.

WHAT WE ARE DOING

As soon as the employee reported the phishing attack to us on January 21, 2021, we immediately notified TravelClick and prevented other users from accessing the phishing email. We also requested that TravelClick immediately cancel the employee's account and create a new account for that user. With that said, up until we received notice from TravelClick on March 11, 2021, we had no reason to believe that any of our guests' personal information was at risk, nor did we know that TravelClick was conducting an investigation into a potential security incident. In response to this incident, we are reviewing our contracts with third-party vendors for hospitality bookings and reevaluating their privacy and security controls to determine whether any updates are necessary.

WHAT YOU CAN DO

Although we have no evidence that your payment card information was actually accessed or misused by an unauthorized third party, we are notifying you out of an abundance of caution. To help alleviate concerns and restore confidence following this incident, we have arranged for you to enroll, at no cost to you, in a comprehensive credit monitoring and identity protection service (*my*TrueIdentity) for two (2) years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution. This service is completely free and will not impact your credit score. You may sign up for this service online or via U.S. mail delivery by following the instructions attached to this notice.

Please also review the enclosed "Other Important Information" document included with this letter for further steps you can take to protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

For further information and assistance, please call our dedicated incident response line at (855) 654-0904 between 8 a.m. – 8 p.m. Central Time, Monday through Friday.

Sincerely,

Ruben Cambero Sedano
General Manager
The American Club

OTHER IMPORTANT INFORMATION

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, you should promptly notify the financial institution or company with which your account is maintained.

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the nationwide credit reporting agencies. To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's (FTC) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Contact information for the national credit reporting agencies for the purpose of requesting a copy of your credit report and other general inquiries is provided below:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213
- **Innovis**, PO Box 1689, Pittsburgh, PA 15230-1689, www.innovis.com, 1-800-540-2505

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the nationwide credit reporting agencies. Contact information for the national credit reporting agencies for the purposes of placing a fraud alert on your file is provided below. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For this reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

- **Equifax**, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com/personal/credit-report-services/credit-fraud-alerts, 1-800-525-6285
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts, 1-800-680-7289
- **Innovis Consumer Assistance**, PO Box 26, Pittsburgh, PA 15230-0026, https://www.innovis.com/personal/fraudActiveDutyAlerts, 1-800-540-2505

Security Freeze. You have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze separately with each of the consumer reporting agencies. To place a security freeze on your credit report, you may do so by contacting each of the consumer reporting agencies through the contact information below:

- **Equifax**, PO Box 105788, Atlanta, GA 30348-5788, www.equifax.com/personal/credit-report-services/credit-freeze, 1-800-298-0045
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html, 1-888-397-3742
- **TransUnion**, PO Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze, 1-888-909-8872
- **Innovis**, PO Box 26, Pittsburgh, PA 15230-0026, www.innovis.com/personal/securityFreeze, 1-800-540-2505

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and may provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit

report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

- **For California Residents**: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.
- **For Iowa Residents**: You are advised to report suspected incidents of identity theft to law enforcement or the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 1-515-281-5926 or 1-888-777-4590.
- **For New York Residents**: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.
- **For North Carolina Residents**: You may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/identity-theft/, by calling 1-877- 566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.
- **For Oregon Residents**: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.
- **For Rhode Island Residents**: You may contact the Rhode Island Attorney General at http://www.riag.ri.gov, by calling 401-274-4400, or by writing to 150 South Main Street, Providence RI 02903. One Rhode Island resident is potentially impacted by this incident. You have the right to file and obtain a copy of any police report. You also have the right to request a security freeze as described above.

Enroll in Credit Monitoring/Identity Restoration Services. As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion® one of the three nationwide credit reporting companies.

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **July 31, 2021**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)