January 17, 2021

Hunter O. Ferguson
600 University Street, Suite 3600
Seattle, WA 98101
D. 206.386.7514
hunter.ferguson@stoel.com

Via Email
(DOJ-CPB@doj.nh.gov)

Consumer Protection and Antitrust Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Breach – McMenamins, Inc.

Dear Members of the Consumer Protection and Antitrust Bureau:

We are counsel to McMenamins, Inc. ("***McMenamins***") in connection with a recent data security incident and write to notify you of this incident and McMenamins' response. Enclosed is a sample copy of the notification letter sent to potentially affected individuals.

McMenamins is a family-owned business that owns and operates a collection of restaurants, brew pubs, hotels, and entertainment venues throughout Oregon and Washington. Currently there are 62 McMenamins locations (52 in Oregon and 10 in Washington).

Nature of the Incident. On December 12, 2021, McMenamins suffered a ransomware attack. After discovering the attack that morning, McMenamins blocked access to its computer systems and contained the attack later that same day. McMenamins promptly began working with an experienced cybersecurity forensics firm to investigate the incident and determine whether any personal information was affected. Based on McMenamins' investigation, it appears that threat actors obtained unauthorized access to McMenamins' systems as early as December 7 and then deployed an encryption malware payload. These actors either accessed or acquired without authorization records containing personal information of: (1) employees as of December 12, 2021; (2) investors; (3) persons previously employed by McMenamins within the July 1, 2010 – December 11, 2021 time period; and (4) at least some persons employed by McMenamins within the January 1, 1998 – June 30, 2010 time period.

Type of Information and Number of Individuals Affected. With respect to both current and previous employees, the records affected include human resources and payroll-

related files containing the following categories of personal information: name, address, telephone number, email address, date of birth, race, ethnicity, gender, disability status, medical notes, performance and disciplinary notes, Social Security number, health insurance plan election, income amount, and retirement contribution amounts. It is possible that files containing direct-deposit bank account information were accessed, but McMenamins does have any indication that such files were, in fact, accessed or acquired.

As to company investors, the following categories of personal information were affected: name, mailing address, email address, and Social Security or Taxpayer Identification number.

On December 15, 2021, McMenamins issued notices of the incident to investors via email, to current employees via email and signs at company locations, and to news media in Oregon and Washington. McMenamins also established a call center to answer questions from potentially affected individuals. Between December 21 and 30, 2021, McMenamins mailed via first-class U.S. mail notices to individuals employed between July 1, 2010 and December 12, 2021, and investors. These notices were mailed to a total of 20,504 known individuals. Of these individuals, 2 had New Hampshire addresses. A sample copy of the notification letter is included in this correspondence.

As noted above, McMenamins' investigation also revealed that the threat actors likely acquired at least some records with personal information of individuals employed between January 1, 1998 and June 30, 2010. Although McMenamins has been able to determine the categories of personal information included in these records as listed above, it has not been able to recover the records themselves or identify the names or contact information of the previous employees actually included in these records. Out of an abundance of caution and for the purposes of providing notice and identity and credit protection and monitoring, McMenamins is assuming that all previous employees during that time period were potentially affected and conservatively estimates that this total does not exceed 20,000. Accordingly, McMenamins also provided substitute notice through its website (mcmenamins.com) and further notification to major statewide media in Washington and Oregon.

Additional Measures Taken in Response to Incident. After discovering the incident on December 12, 2021, McMenamins took the actions referenced above. It also promptly engaged an experienced cybersecurity forensics firm and has been working to investigate the source and scope of the attack, restore its business systems, and enhance its security. McMenamins reported the incident to the Federal Bureau of Investigation ("***FBI***") and has been cooperating with the FBI's investigative efforts. McMenamins is providing all of the affected individuals referenced above with identity and credit monitoring and protection services through Experian. Information about these services is included in the mailed notices and substitute notice on McMenamins' website as well as the media notices. McMenamins also notified the three major credit reporting bureaus.

Contact Information. McMenamins remains dedicated to protecting personal information in its control. If you have any questions or need additional information, please contact me at 206.386.7514 or hunter.ferguson@stoel.com.

Very truly yours,

Hunter O. Ferguson

Enclosure: Sample Notification Letter

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

December 30, 2021

H3037-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

DATA BREACH NOTIFICATION

Dear Sample:

As you might have learned, McMenamins experienced a cyberattack in early December 2021. We have determined that this attack may have affected your personal information in company records relating to persons previously employed with McMenamins between July 1, 2010, and December 11, 2021. This letter explains the incident, your information potentially affected, and how you can protect yourself, including identity and credit protection services that we are providing to you.

***WHAT HAPPENED*.** On December 12, 2021, McMenamins suffered a ransomware attack. As soon as we realized what was happening, we blocked access to our systems to contain the attack that day. Cybercriminals deployed malicious software on the company's computer systems that prevented us from using these systems and the information they contain.

***WHAT INFORMATION WAS INVOLVED*.** We have determined that the hackers stole certain business records, including human resources/payroll data files for previous employees. These files contain the following categories of employee information: name, address, telephone number, email address, date of birth, race, ethnicity, gender, disability status, medical notes, performance and disciplinary notes, Social Security number, health insurance plan election, income amount, and retirement contribution amounts. It is possible that the hackers accessed or took records with direct-deposit bank account information, but we do not have any indication that they did, in fact, do so.

***WHAT WE ARE DOING*.** We are investigating this incident and working to get business back online. We notified the FBI and are cooperating with their efforts. We are working with an experienced cybersecurity investigation firm to understand the attack, restore our systems, and enhance our security. We have notified the Attorney Generals of Oregon and Washington, major credit reporting bureaus, and the news media. If we learn additional information affecting you, we will provide further notice.

***WHAT YOU CAN DO TO PROTECT YOUR INFORMATION*.** You should be vigilant when responding to communications from unknown sources and regularly monitor your financial accounts and healthcare information for any unusual activity. If you notice any unusual activity, you should immediately notify your financial institutions (*e.g.*, your bank) and your health insurer. A set of recommendations for identity theft protection and details on how to place a fraud alert or a security freeze on your credit file is enclosed. If you suspect that you are the victim of identity theft or fraud, you should notify your state Attorney General's Office and the Federal Trade Commission. These agencies' contact information is enclosed.

To help protect your identity, we are providing a ##-month membership of Experian's® IdentityWorks℠. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow these steps:

- Ensure that you **enroll by**: **March 31, 2022.** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit.
- Provide your **activation code**: **ABCDEFGHI**

If you have questions, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 401-0552 by March 31, 2022. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian. This call center can also answer questions you might have about the incident.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You will receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:**** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (**888) 401-0552**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for [coverage length] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. This site also has self-help tips and information about identity protection.

We sincerely apologize again for this incident. We know that the past two years have been very hard on all of our employees, and we are committed to providing you with assistance and support. If you have questions regarding this matter, please contact the call center at (**888) 401-0552**.
Sincerely,

Mike McMenamin
President

Brian McMenamin
Vice President/Secretary

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

IDENTITY THEFT PREVENTION AND PROTECTION

Monitor Your Accounts and Credit Reports, and Notify Police and the FTC of Suspicious Activity:
When you receive account statements, credit reports, and monitoring alerts, review them carefully for unauthorized activity. Look for accounts you did not open, unauthorized purchases, inquiries from creditors that you did not initiate, and personal information that you do not recognize, such as a home address or Social Security number. If you have concerns, call your bank, the account provider, or the credit reporting agency. If possible, place a security verification secret word, similar to a password, on your accounts.

If you suspect any fraudulent activity or identity theft, promptly report it to local law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a complaint with the FTC, go to https://www.consumer.ftc.gov/features/feature-0014-identity-theft or call 1-877-ID-THEFT (877-438-4338). Request copies of any police or investigation reports created, as you might need to provide this information to credit reporting agencies or to supposed creditors to clear up your records.

***Obtain Free Credit Reports*:** Even if you do not find any signs of fraud on your reports, you should check your credit report regularly. There are three main credit reporting agencies: Equifax, Experian, and TransUnion. Their contact information, along with contact information for the FTC and some state agencies, are on the reverse side of this tip sheet. Each credit reporting agency must provide you annually with a free credit report, at your request made to a single, centralized source for the reports, AnnualCreditReport.com. You are not required to order all three reports at the same time; instead, you may rotate your requests so that you can review your credit report on a regular basis. In addition, many states have laws that require the credit reporting agencies to provide you with a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

***Free Services by Credit Reporting Agencies*:** Each credit reporting agency offers additional free services to help you protect your credit. TransUnion at www.transunion.com permits you to sign up for TrueIdentity which is a service that allows you to examine your TransUnion credit file and place a "credit lock" which prevents others from opening up credit in your name. Experian at www.experian.com provides you with a free credit report every month when you select "Start with your free Experian Credit Report." Equifax at www.equifax.com permits you to sign up for "Lock & Alert" which also allows you to place a credit lock.

***Fraud Alert*:** You may ask the credit reporting agencies to place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three credit reporting agencies. As soon as that agency processes your fraud alert, it is supposed to notify the other two, which then also must place fraud alerts in your file. An *initial fraud alert* stays in your file for at least 90 days. An *extended alert* stays in your file for seven years. To place either of these alerts, a credit reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency.

Security Freeze: You also have the right to place a security freeze on your credit report at any of the three main credit reporting agencies. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request. If you choose to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail, the following information must be included when requesting a security freeze: (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. 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, and displays your name, current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the agency. The main three credit reporting agencies provide details about their security freeze services and state requirements at the following links:

- Experian: http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/
- Equifax: https://help.equifax.com/app/answers/detail/a_id/75/~/security-freeze-fees-and-requirements
- TransUnion: https://www.transunion.com/credit-freeze/place-credit-freeze

***Internal Revenue Service*:** Tax-related identity theft is when someone uses your Social Security number to file a false tax return claiming a fraudulent refund. If you received IRS correspondence indicating you may be a victim of tax-related identity theft or your e-file tax return was rejected as a duplicate, do the following:

- Submit an IRS Form 14039, Identity Theft Affidavit, to the IRS;
- Continue to file your tax return, even if you must do so by paper, and attach the Form 14039; and
- Watch for any follow-up correspondence from the IRS and respond quickly.

The fillable IRS Form 14039 is available at IRS.gov. Follow the instructions exactly. You can fax or mail it or submit it with your paper tax return if you have been prevented from filing because someone else has already filed a return using your SSN. You only need to file it once. Do not respond to threats made over the phone or via email that the IRS will take action against you. The IRS will communicate with you in writing.

***Financial Accounts, Oral Passwords, and MFA*:** If financial accounts are affected, contact the institution and ask them about steps you may take to further protect your account. Financial institutions will often permit you to place an oral password on your account or enable multifactor authentication to your online account. You also should implement multifactor authentication controls, when available, for personal accounts such as your email account, online banking, online bill pay services, and other accounts you intend to be secure. For more information about MFA, you can review various online explanations, including https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661.

***Contact Information for the FTC, Credit Reporting Agencies, and State Consumer Protection Agencies*:** If you suspect fraudulent activity on any of your financial accounts (savings, checking, credit card) or identity theft, you are encouraged to report your concerns to your financial institutions and the relevant agencies below.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft/

Oregon Attorney General
Consumer Protection
1162 Court St. NE
Salem, OR 97301-4096
1-877-877-9392
https://www.doj.state.or.us/consumer-protection/

Washington Attorney General
Consumer Protection
800 5th Avenue, Suite 2000
Seattle, WA 98104-3188
1-800-551-4636
https://www.atg.wa.gov/guardit.aspx

AnnualCreditReport.com
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
www.annualcreditreport.com

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 34012
Fullerton, CA 92834
1-800-680-7289
www.transunion.com