McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins LLC
300 N. LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

Nicholas A. Kurk
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com

November 22, 2023

VIA PORTAL

Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Midwest Gaming & Entertainment, LLC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Midwest Gaming & Entertainment, LLC, d/b/a Rivers Casino Des Plaines ("Rivers Casino"). I am writing to provide notification of an incident at Rivers Casino that may affect the security of personal information of Maine residents. By providing this notice, Rivers Casino does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

On August 12, 2023, Rivers Casino became aware of suspicious activity on its systems involving a potential ransomware incident. Upon identifying the activity, Rivers Casino acted quickly to contain the threat, investigate, and ensure the security of its systems with the assistance of third-party forensic specialists. The investigation revealed that an unauthorized actor gained access to Rivers Casino's systems on or around August 12, 2023, and as a result likely obtained some information. On November 2, 2023, after an extensive forensic investigation and review, Rivers Casino discovered that certain personal information of approximately two hundred and two (202) Maine residents was included within the files that were subject to unauthorized access or acquisition as a result of the incident. Further, on November 14, 2023, Rivers Casino located the most recent contact information for these individuals.

The personal information contained within the impacted data included first and last name, driver's license and/or government ID number, financial account number, and Social Security number. The types of impacted information varied by individual.

Rivers Casino has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, Rivers Casino wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Rivers Casino is providing the affected residents with notification of this incident, commencing on or about November 20, 2023. The notice will be in

substantially the same form as the letter attached hereto. In addition, Rivers Casino is providing substitute notice, consisting of a website posting and media notice to one or more media outlets in this state. Rivers Casino is also offering the affected residents whose Social Security number was potentially impacted by the incident with complimentary one-year membership with a credit monitoring service. Rivers Casino is advising the affected residents to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. Rivers Casino is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected residents are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Rivers Casino, protecting the privacy of personal information is a top priority. Rivers Casino is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Rivers Casino continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com.

Very truly yours,

Nicholas A. Kurk

Encl.

[redacted]

Dear [redacted]

One of our top priorities is the safety and security of our customers and Team Members, including protecting the personal data we maintain about them. While Rivers Casino Des Plaines utilizes robust security protocols, unfortunately, we recently discovered a data security incident. Upon learning of the incident, Rivers promptly took steps to contain the threat and secure our systems, avoiding any interruption to our operations or in the services we provide to our customers. Rivers also engaged third-party cybersecurity support to investigate the incident. Although we have no evidence of financial fraud or identity theft related to this data, in accordance with applicable law, we wanted to provide you with information about the incident, resources, and steps that you may take to help protect your personal information, should you feel it appropriate to do so.

What Happened?

While our operations were not impacted, Rivers determined that this incident involved unauthorized access to our network. Specifically, on November 2, 2023, we determined that files containing certain personal information of Rivers Casino Des Plaines Team Members, customers, and online sportsbook customers may have been accessed or removed from our network as a result of this incident on or around August 12, 2023. We have not identified any indication that the networks of any other Rivers casinos were accessed during this incident. Further, no Betrivers online or mobile gaming platform, operations or systems were compromised or breached.

What Information Was Involved

The impacted files contained your [redacted]

What We Are Doing

We promptly engaged third-party cybersecurity support to assist with containing the incident and to help ensure the security of our systems. Further, we immediately launched an investigation in consultation with law enforcement and outside cybersecurity professionals to determine the nature and scope of the incident.

What You Can Do

As previously stated, we have no indication of financial fraud or identity theft related to this incident. However, out of an abundance of caution and to help protect you from potential misuse of your information, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. For more information on identity theft prevention and Experian IdentityWorks℠ Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to help protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant against incidents of identity theft and fraud and review your financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Rivers values the trust and loyalty of its customers and Team Members and we share in any frustration this incident may cause.

If you have any questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted], excluding major U.S. holidays.

Sincerely,

Midwest Gaming & Entertainment, LLC d/b/a Rivers Casino Des Plaines
3000 S. River Road
Des Plaines, IL 60018

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at [redacted]
or call [redacted] to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted].

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

You may also place a "Security Freeze" on your credit file, at no charge. A security freeze prohibits, with certain exceptions, the consumer reporting agencies from releasing any information from your credit report without your written authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting agencies using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

After receiving your freeze request, each credit reporting agency will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting agencies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies, such as accounts you did not open or inquiries from creditors that you did not authorize, and verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, such as to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report to provide to creditors should you need to contest fraudulent activity.

You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: 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: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and help ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There were [redacted] Rhode Island residents impacted by this incident.