

EXHIBIT 1

By providing this notice, UP Entertainment does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 19, 2021, UP Entertainment became aware of suspicious activity in its computer network. Upon learning of the activity, UP Entertainment immediately took steps to secure its network and minimize any disruption to their operations and launched an investigation into the nature and scope of the incident with the assistance of industry-leading cybersecurity specialists, who determined that UP Entertainment was the victim of a malware attack. Although the investigation determined that certain systems containing information were accessed, it was not able to determine whether any specific file or information was actually accessed. Therefore, UP Entertainment is engaging in a comprehensive review of the impacted systems to determine the information that was present on them at the time of the incident. While this review is ongoing, UP Entertainment's investigation recently confirmed that certain information that could have been subject to unauthorized access as a result of this incident includes name, address, Social Security number, and passport. The impacted information is not the same for all individuals.

Notice to Maine Resident

On or about September 14, 2021, UP Entertainment began providing written notice of this incident to affected individuals, which includes one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. Notification to impacted individuals is ongoing, and UP Entertainment may supplement this notification if it is determined that a significant amount of additional Maryland residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, UP Entertainment moved quickly to investigate and respond to the incident, assess the security of UP Entertainment systems, and notify potentially affected individuals. UP Entertainment is also working to implement additional safeguards and training to its employees. UP Entertainment is providing complimentary access to credit monitoring services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident.

Additionally, UP Entertainment is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A



UP Entertainment Inc.
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

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

September 14, 2021

Dear <<First Name>> <<Last Name>>,

UP Entertainment is writing to make you aware of an incident that may affect the security of some of your information. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident, our ongoing response, and resources available to you right now to help protect your information, should you feel it is appropriate to do so

What Happened? On May 19, 2021, UP Entertainment became aware of suspicious activity in our computer network. We immediately took steps to secure our network and minimize any disruption to our operations and launched an investigation into the nature and scope of the incident with the assistance of industry-leading cybersecurity specialists, who determined that UP Entertainment was the victim of a malware attack. Although our investigation is ongoing to confirm the full nature and scope of the incident, we wanted to share this information with you out of an abundance of caution.

What Information Was Involved? Although our investigation determined that certain systems containing proprietary information systems were accessed, it was not able to determine whether any specific file or information was accessed. Therefore, we are engaging in a comprehensive review of these systems to determine the information that was present on them at the time of the incident. Our investigation to date determined your information may have been impacted by this incident and includes your name, <<Variable Text 1>>.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems. We are continually reviewing existing security policies and have implemented additional cybersecurity measures to further protect against similar incidents moving forward. We reported this incident to law enforcement and are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for <<Variable Text 2>> months at no cost to you, through IDX. You can find information on how to enroll in these services in the below *“Steps You Can Take to Protect Your Information.”* We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed *“Steps You Can Take to Help Protect Your Information.”*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-800-939-4170, Monday through

Friday, 9 am to 9 pm ET. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Charley Humbard". The signature is written in a cursive, flowing style with a large initial "C".

Charley Humbard
Chief Executive Officer
UP Entertainment, LLC

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is December 14, 2021.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items 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 our ID Care team who will help you determine the cause of the suspicious items. In the unlikely 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.

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. 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.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, 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 security 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a 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. Please note that in order to file a report with law enforcement 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 Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.