



MULLEN
COUGHLIN, LLC
ATTORNEYS AT LAW

STATE OF NH
DEPT OF JUSTICE

2019 SEP -9 PM 12:47

Paul T. McGurkin, Jr.
Office: 267-930-4788
Fax: 267-930-4771
Email: pmcgurkin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

September 5, 2019

VIA U.S. 1st CLASS MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Feld Entertainment, Inc. ("Feld") located at 800 Feld Way, Palmetto, Florida, 34221 and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. By providing this notice, Feld does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

Earlier this year, Feld learned of suspicious activity involving certain employee email accounts related to a phishing scam. Feld immediately launched an investigation and began working with third-party forensic experts to determine the nature and scope of this incident. This investigation confirmed unauthorized access to certain Feld employee accounts on separate occasions between November 14, 2018 and January 25, 2019. Upon learning of the unauthorized access, Feld began both a programmatic and manual review of the complete contents of the each of the email accounts subject to unauthorized access. On April 22, 2019, the vendor's preliminary review to determine the types of personal information in the accounts and to whom the information related was completed. However, the information provided by the vendor was insufficient to move forward with notice. Feld immediately began an internal review of its records to identify potentially affected individuals and address information in order to provide notice of this incident. On June 27, 2019, this investigation was completed and determined the types of personal information present within the email account included name, and passport number. To date, Feld has no evidence of any actual or attempted misuse of the personal information within the affected email accounts.

Notice to New Hampshire Resident

On September 5, 2019, Feld began providing written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

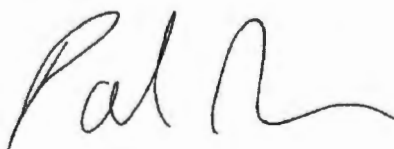
Upon discovering the event, Feld moved quickly to investigate and respond to the incident, reset the passwords of the impacted accounts, assess the security of Feld's systems, and notify potentially affected individuals. Feld is also working to implement additional safeguards and training to its employees including multi-factor authentication.

While Feld is not aware of any attempted or actual misuse of personal information, Feld is also providing access to credit monitoring services for two (2) years, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, Feld is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Feld is 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,



Paul T. McGurkin of
MULLEN COUGHLIN LLC

PTM:ara
Enclosure

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Feld Entertainment, Inc. ("Feld") is writing to inform you of a recent incident out of an abundance of caution because some of your information may have been affected. We write to provide you with information about the incident, steps taken since discovering the incident, and information on what you can do to better protect against the possibility of identity theft and fraud.

What Happened? Earlier this year, Feld learned of suspicious activity related to certain employee email accounts as a result of a phishing scam. Feld immediately launched an investigation and began working with third-party forensic experts to determine the nature and scope of this incident. This investigation confirmed unauthorized access to certain email accounts on separate occasions between November 14, 2018 and January 25, 2019. Please note that it is not possible to determine what, if anything, was actually viewed during the unauthorized access. Nonetheless, Feld began a programmatic and manual review of the complete contents of the email accounts subject to unauthorized access to determine what content was in those accounts. On April 22, 2019, the vendor's preliminary review was completed. Feld immediately began an internal review of its records to identify the affected individuals and address information in order to provide notification to potentially affected individuals. This research and review of the content was fully completed on June 27, 2019, and it was determined during that review that protected information relating to you was identified as part of the content.

What Information Was Involved? While the investigation was unable to definitively confirm whether any emails or attachments were accessed, Feld is notifying you in an abundance of caution because some of your information was present within one of the impacted email accounts. The information potentially affected includes your <<b2b_text_1>>. To date, Feld has not received any reports of actual or attempted misuse of this information.

What We Are Doing. We take this incident and the security of the personal information in our care very seriously. Feld shut down the initial incident within hours of detection, and immediately changed employee passwords. Since discovering the event, we quickly began working to determine what the scope of the incident was, and what additional precautions and actions could be taken to protect against future criminal conduct. This is in addition to Feld's existing policies and procedures already in place to safeguard and to secure the information in our systems.

As an added precaution, Feld is also offering complimentary access to twenty four (24) months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

What You Can Do. While we are unaware of any actual or attempted misuse of your information, you can find out more about how to help protect against potential identify theft and fraud in the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*. There you will also find more information on the identity monitoring services and how to activate them.

For More Information. We understand that you may have questions about this letter. If have any questions, please call our dedicated assistance line at [1-800-877-7777](tel:1-800-877-7777) between the hours of 8:00 a.m. and 5:30 p.m., Central Time, Monday through Friday.

We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink, appearing to read "Stephen Payne". The signature is fluid and cursive, with a long horizontal stroke at the end.

Stephen Payne
VP of Public Affairs

Steps You Can Take to Protect Against Identity Theft and Fraud

Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit enroll.idheadquarters.com to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Additional Steps

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	Equifax PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services
---	---	---

In order to request a security freeze, you will 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. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	Equifax P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services
---	---	--

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, 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 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. We encourage you to 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.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [There is one Rhode Island resident impacted by this incident.](#)



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.