Lewis Bess
Williams & Weese P.C.

STATE OF NH
DEPT OF JUSTICE
2017 MAR 27 AM 11: 36

Deborah Shinbein Howitt
EMAIL dhowitt@lewisbess.com
DIRECT 303.228.2502
WEB www.lewisbess.com

1801 California Street
Suite 3400
Denver, Colorado 80202
MAIN 303.861.2828
FAX 303.861.4017

March 23, 2017

VIA FIRST CLASS MAIL

Joseph Foster
Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Foster:

I am writing to inform you of an information security breach suffered by Goldenvoice, including information collected at and in connection with The Coachella Valley Music and Arts Festival, the Stagecoach Festival, and through the Coachella.com website.

What Happened?
This incident relates to the unauthorized acquisition, by hackers, of certain information collected in connection with the 2016 Coachella Music and Arts Festival, the 2016 Stagecoach Festival, and through the Coachella.com website. The hackers are believed to have accessed the information described below from September 2016 to late February 2017. We initially became aware of the security incident on February 21, 2017 and we immediately opened an investigation, notified law enforcement and engaged a leading forensic IT firm, however we did not understand the full scope of the incident (and the data affected) until early March. The incident was contained and the unauthorized access terminated shortly after the investigation began and the relevant security vulnerability has been mitigated.

What Information Was Involved?
The information potentially affected by this security incident varies based on the individual, whether they purchased a ticket or registered on the website, and the information they chose to provide. If an individual was a registered user of the Coachella.com website, the affected information may include first and last name; Coachella.com username; email address; birth date; and phone number (if provided). If the individual provided information to us for the delivery or pickup of a Coachella or Stagecoach ticket or wristband, the affected information may also include mailing address and information relating to identification documents provided when the individual picked up or claimed a wristband at the festival (if any). Our investigation indicates that the hackers did not have access to any payment or financial information, nor users' account passwords.

What We Are Doing.
We continue to investigate the security incident, in partnership with law enforcement and independent computer forensic investigators, to learn more and prevent a similar issue from occurring in the future. Though the relevant security vulnerability has been remediated, we will continue to monitor the situation closely for any additional suspicious activity. Furthermore, we have applied important security updates to our systems and taken other proactive measures to help safeguard our services and protect your personal information. As an added precaution, we have arranged for identity theft protection at no cost to qualifying US individuals whose driver's license, passport number, or other identification information was affected.

Notification and Number of Residents Affected

We believe that two (2) residents of the state of New Hampshire were affected by this breach. Where possible, these residents will be notified via first class U.S. mail, sent on or after the date of this letter above (as appropriate). A copy

of the form letter mailed to the affected residents is attached to this letter. For individuals whose state of residence could not be determined, and for whom contact information was insufficient to send notice via first class mail, notice will be provided via email to the individual (if available), to news media, and through a public notice on the Goldenvoice website.

Contact

If you have any questions you may contact me at dhowitt@lewisbess.com or 303.861.2828.

Sincerely,

Deborah Howitt

Deborah Howitt

Exhibit 1 – Template Notice to Consumers (Latest Draft)

[SEE ATTACHED]

GOLDENVOICE

Processing Center • P.O. BOX 141578 • Austin, TX 78714

STATE OF NH
DEPT OF JUSTICE
2017 MAR 27 AM 11:36

00001
ACD1234

00001
Sample
1234 MAIN STREET
ANYTOWN US 12345-6789

March 22, 2017

Notice of Data Breach

Dear Sample,

Goldenvoice and The Coachella Valley Music and Arts Festival take the privacy and security of our fans' personal information seriously. Accordingly, we are writing to inform you of a security incident that may have affected certain personal information you provided to us. You are receiving this letter because you are part of a limited group of festival attendees who provided some form of identification when you picked up your festival wristband in person.

Please see below under "What We Are Doing" for information on identity protection services we are making available to you at no charge, through AllClear ID. Additional resources are provided on the enclosed page.

What Happened?

This incident relates to the unauthorized and illegal acquisition, by criminal hackers, of certain information collected in connection with the 2016 Coachella Music and Arts Festival and through the Coachella.com website. The criminal hackers are believed to have accessed this information during the period of September 2016 to February 2017. As soon as we became aware of the security incident, we immediately opened an investigation, notified law enforcement and engaged a leading forensic IT firm. Shortly thereafter, the security vulnerability was remediated and the security incident has been fully contained.

What Information Was Involved?

The information potentially affected by this security incident may include some combination of your first and last name; Coachella.com username; email address; mailing address; birth date; phone number (if provided); and driver's license number, passport number, or other ID you used when you picked up your wristband at the festival. Our investigation indicates that the individuals did not have access to any payment or financial information, nor any of your passwords.

What We Are Doing.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-263-7376 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at GV.allclearid.com.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We continue to investigate the security incident, in partnership with law enforcement and independent computer forensic investigators, to learn more and prevent a similar issue from occurring in the future. Though the security vulnerability has been remediated, we will continue to monitor the situation closely for any additional suspicious activity. Furthermore, we have applied important security updates to our systems and taken other proactive measures to help safeguard our services and protect your personal information.

What You Can Do.

To help protect the security of your information, you can sign up for AllClear ID services as described above. In addition, please closely monitor your online and financial accounts, and be aware that criminals may attempt to send you targeted emails seeking to obtain other confidential information from you (i.e. phishing scams), or may otherwise try to use your personal information.

Let us know if you see any suspicious activity on your Coachella account, and always report any illegal activities to law enforcement or an appropriate government authority (see below for helpful resources). If you notice any unauthorized or suspicious financial activity, such as new credit applications, loans, or account openings, report it to the appropriate financial institution in addition to government authorities. Remember, Coachella will never ask for your username, password, or other sensitive personal information via email. If you receive an email from us requesting this information, do not open any attachments and do not provide any personal information. If you have concerns or suspicions about an email from Coachella, Goldenvoice, or any of our other festivals, please contact us at info@coachella.com.

Although our investigation indicates that Coachella account passwords were not affected, consider taking a moment to change any old, reused, or insecure passwords and remember to follow appropriate security practices when managing your online accounts. More information on creating strong passwords can be found on the Department of Homeland Security's website: https://www.us-cert.gov/ncas/tips/ST04-002.

For More Information.

If you have any questions regarding this notice or if you would like more information, please do not hesitate to contact us at info@coachella.com or call AllClear ID at 1-855-263-7376.

Most importantly, we sincerely regret any concern this security incident may cause. Our fans are the most important part of Coachella, and we value your trust and understanding.

Sincerely,

Skip Paige
Vice President, Goldenvoice

IMPORTANT INFORMATION ABOUT IDENTITY THEFT PROTECTION

Please sign up for identity protection services through AllClear ID, as described in the notification letter under "What We Are Doing." This service is offered at no cost to you. Additional information and resources are provided below.

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report, or request information on how to place a fraud alert or security freeze on your credit file, by contacting any of the national credit bureaus below. Remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. The contact information for three major credit bureaus are as follows:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19022 1-800-888-4213 www.transunion.com

Contact Information for the Federal Trade Commission
In addition to the credit bureaus above, you may contact or visit the website of the Federal Trade Commission to learn more about how to protect yourself against identity theft, or how to place a fraud alert or security freeze on your credit file. The contact information for the FTC is as follows:

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

How to Place a Fraud Alert on Your Credit File
To protect yourself from the possibility of identity theft or other fraud, you may place a fraud alert on your credit file. The fraud alert helps to prevent someone else obtaining credit in your name. If you have a fraud alert on your credit file, creditors will contact you and verify your identity before they open any new accounts or change your existing accounts, but it should not affect your credit score or your ability to obtain new credit (although it may cause a delay in any applications or approvals). As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts, so you do not need to place alerts with more than one of the credit bureaus. To place a fraud alert, go to any of the following links and complete the requested steps:

https://www.experian.com/fraud/center.html
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page

How to Place a Security Freeze on Your Credit File
If you wish to take more extensive measures to prevent new credit being opened in your name, you may consider placing a security freeze on your credit file. You should only place a security freeze if you want to prevent most parties from obtaining your credit report and prevent all credit, loans and related services from being approved in your name without your consent. Please consider that this may also impact or delay your ability to obtain certain government services, rental housing, employment, cell phone plans, insurance, utilities, and other services.

You will need to apply for a security freeze separately with each of the credit bureaus. The requirements to obtain a security freeze vary depending on your state of residence, and you may be required to pay a fee, provide your name and social security number, copies of important identification records (including a list of addresses, copies of government issued IDs, and/or utility bills), provide an incident report if you are a victim of identity theft, or take other measures as described on the credit bureaus' websites. You may need to follow these steps for each individual (such as a spouse or dependent)

who will request a security freeze. You can find more information regarding a security freeze at the following links, or by calling each of the credit bureaus at the numbers listed in this notification letter:

https://www.freeze.equifax.com
https://www.experian.com/consumer/security_freeze.html
http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Contact Information for State Government Agencies
You may also contact your state's attorney general or state department of revenue, as there may be more information available at the state level. Residents of California, Rhode Island, Maryland, and North Carolina are advised that they may contact their local law enforcement agencies using the following contact information:

Rhode Island Office of the Attorney General Consumer Protection Unit 150 South Main Street Providence, RI 02903 Telephone: (401) 274-4400 http://www.riag.ri.gov	**North Carolina Attorney General's Office** 9001 Mail Service Center Raleigh, NC 27699-9001 Telephone: (919) 716-6400 Fax: (919) 716-6750
Maryland Office of the Attorney General Identity Theft Unit 200 St. Paul Place, 16th Floor Baltimore, MD 21202 Phone: (410) 576-6491 Fax: (410) 576-6566 E-mail: idtheft@oag.state.md.us	**California Attorney General's Office** California Department of Justice Attn: Office of Privacy Protection P.O. Box 944255 Sacramento, CA 94244-2550 Tel: (916) 322-3360 Toll-free: (800) 952-5255 https://oag.ca.gov/idtheft