Debevoise & Plimpton

Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
+1 212 909 6000

By Electronic Mail

September 2, 2020

Consumer Protection Division
Office of the Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

To Whom It May Concern:

On behalf of Warner Music Group ("WMG"), and consistent with Iowa Code Ann. § 715C.2, this letter provides notice of a computer data security incident. Although our investigation is ongoing, based on currently known information, WMG believes approximately 967 potentially affected individuals reside in your state.

WMG is a music entertainment company that also sells merchandise on behalf of a number of bands and artists with which it works. On August 5, 2020, WMG learned that an unauthorized third party had compromised a number of US-based e-commerce websites that WMG operates but that are hosted and supported by an external service provider. This allowed the unauthorized third party to potentially acquire a copy of information customers entered on the affected websites after placing an item into their shopping carts. This could have impacted purchases made with credit cards from the affected websites between April 25, 2020 and August 5, 2020. The information compromised could have included the individual's name, email address, telephone number, billing address, shipping address, and payment card details (card number, CVC/CVV and expiration date).

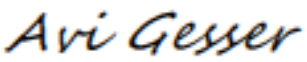
Upon discovering the incident, WMG immediately launched a thorough forensic investigation with the assistance of leading outside cybersecurity experts and promptly took steps to address and correct the issue. WMG continues to conduct daily scans to monitor for any suspicious activity and, at this time, WMGs believe that the third party's unauthorized access has been eliminated. WMG also notified the relevant card providers as well as law enforcement, and is continuing to work with both the card providers and law enforcement.

While WMG cannot definitively confirm which individuals' data was potentially acquired by the unauthorized third party, WMG is in the process of notifying potentially affected customers in accordance with applicable legal requirements, including all Iowa residents who placed an order on one of the affected websites during the period of compromise. WMG anticipates sending notices via U.S. Mail beginning on or about September 3, 2020. A sample customer notification letter is attached. To protect individuals further, WMG has engaged Kroll Information Assurance, LLC, to provide 12

months of free credit monitoring and identity theft protection services to individuals whose personal information may have been acquired by the unauthorized third party.

WMG takes the protection of its customers' data seriously, and is committed to answering any questions your office may have. Please do not hesitate to contact me at the address above, at 1-212-909-6577, or agesser@debevoise.com.

Yours sincerely,



Avi Gesser

Partner

WARNER MUSIC GROUP

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

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

NOTICE OF DATA BREACH

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

We are writing to let you know that a cybersecurity incident involving a number of e-commerce websites operated by Warner Music Group ("WMG") through an external service provider may have allowed an unauthorized third party to acquire a copy of personal information you entered into those websites. We want to emphasize at the outset that keeping personal information safe and secure is very important to us, and we deeply regret that this incident has occurred.

WHAT HAPPENED?

On August 5, 2020, we learned that an unauthorized third party had compromised a number of US-based e-commerce websites WMG operates but that are hosted and supported by an external service provider. This allowed the unauthorized third party to potentially acquire a copy of the personal information you entered into one or more of the affected website(s) between April 25, 2020 and August 5, 2020.

While we cannot definitively confirm that your personal information was affected, it is possible that it might have been as your transaction(s) occurred during the period of compromise. If it was, this might have exposed you to a risk of fraudulent transactions being carried out using your details.

WHAT INFORMATION WAS INVOLVED?

Any personal information you entered into one or more of the affected website(s) between April 25, 2020 and August 5, 2020 after placing an item in your shopping cart was potentially acquired by the unauthorized third party. This could have included your name, email address, telephone number, billing address, shipping address, and payment card details (card number, CVC/CVV and expiration date).

Payments made through PayPal were not affected by this incident.

WHAT WE ARE DOING

Upon discovering the incident we immediately launched a thorough forensic investigation with the assistance of leading outside cybersecurity experts and promptly took steps to address and correct the issue. We also notified the relevant credit card providers as well as law enforcement, with whom we continue to cooperate.

To protect you further, we are offering identity monitoring services through Kroll for 12 months, free of charge. You can find further details below on how to sign up.

WHAT YOU CAN DO

We strongly encourage you to take advantage of the identity monitoring services we are offering and to remain vigilant for any unauthorized use of your payment cards or suspicious email communications, particularly those purporting to come from Warner Music Group or any WMG-related websites.

If you identify any potentially suspicious transactions or other indications of identity theft, you should contact the relevant bank or card provider as soon as possible. Please also find enclosed additional steps that you can take to protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

CREDIT 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 one year. 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 **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **December 11, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

FOR MORE INFORMATION

We sincerely regret that this incident has occurred and are very sorry for any inconvenience or concern it may have caused you. If you have any questions about the incident, please contact us at 1-866-951-4190, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time or data.protection@warnermusic.com.

Warner Music Group

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

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

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian:**	**TransUnion:**
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
866-349-5191	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 reports to be

provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For New York residents: You may contact the Office of the New York Office of the Attorney General, The Capitol, Albany NY 12224-0341, https://www.ag.ny.gov/, 1-800-771-7755.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Colorado, Georgia, Maine, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For Tennessee residents:

TENNESSEE CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

You have a 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. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you are actively seeking a new credit, loan, utility, or telephone account, you should understand that the procedures involved in lifting a security freeze may slow your applications for credit. You should plan ahead and lift a freeze in advance of actually applying for new credit. When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a 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 personal identification number or password;

(2) Proper identification to verify your identity; and

(3) The proper information regarding the period of time for which the report shall be available.

A consumer reporting agency must authorize the release of your credit report no later than fifteen (15) minutes after receiving the above information.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information in your credit report for the purposes of fraud control, or reviewing or collecting the account. Reviewing the account includes activities related to account maintenance.

You should consider filing a complaint regarding your identity theft situation with the federal trade commission and the attorney general and reporter, either in writing or via their web sites.

You have a right to bring civil action against anyone, including a consumer reporting agency, which improperly obtains access to a file, misuses file data, or fails to correct inaccurate file data.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll'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.