

Colman McCarthy

October 3, 2024

2555 Grand Blvd.
Kansas City, MO 64108
dd 816.559.2081
cdmccarthy@shb.com

Via Email to idtheft@oag.state.md.us

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

RE: Universal Music Group Security Incident

To Whom It May Concern:

On behalf of Universal Music Group (“UMG”), I am writing to inform your office about a security incident that affected four Maryland residents. The incident involved unauthorized access to personal information stored in a data repository. UMG has notified the affected individuals and, in that notice, provided instructions for activating complimentary credit monitoring.

In July 2024, UMG detected an incident involving unauthorized activity in one of its internal applications. UMG’s outside counsel engaged a leading forensic firm to conduct a forensic investigation. The investigation, which is ongoing, found that an unknown third party had gained unauthorized access to a platform UMG uses for the storage and development of source code. The third party used that access to acquire credentials for a limited number of other UMG applications and data repositories. After identifying the impacted data that could potentially contain personal information, UMG engaged a data review firm to assess the contents of those files. UMG received those results on August 30, 2024.

UMG, in coordination with outside counsel, promptly began reviewing that report to assess notification obligations and locate addresses for impacted individuals. The report showed that the third party acquired files with the following types of personal information: name and Social Security number. In some cases, an individual’s birthdate and address were also in the impacted files. Based on those results, UMG mailed notice to affected individuals on October 3, 2024. The company included an offer for complimentary credit monitoring in those notices. A copy of that notice is attached.

In addition to providing notice, UMG took additional steps to promptly address this incident. The company opened an investigation upon detecting potential unauthorized activity in its environment. The company then engaged legal experts to advise on the company’s responsibilities, IT forensic experts to investigate the incident, and a data-review company to analyze the potentially

impacted data. UMG also adopted measures to bolster security, such as: increasing logging, strengthening access controls, moving more systems to the internal network, expanding the use of multifactor authentication, and adopting additional data loss prevention tools.

October 3, 2024
Page 2

If you have any questions, you can contact me at: cdmccarthy@shb.com or 816-559-2081.

Sincerely,

A handwritten signature in black ink, appearing to read 'Colman McCarthy', with a stylized flourish at the end.

Colman McCarthy
Partner



UNIVERSAL MUSIC GROUP
Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741



October 3, 2024

NOTICE OF DATA BREACH

Dear [REDACTED]:

We are sending you this notice because Universal Music Group (“UMG”) experienced a data breach that affected some of your personal information. While we have found no evidence that your information has been misused, we are informing you of the incident to allow you to take steps to maintain the security of your identity.

WHAT HAPPENED?

In early July, we detected unauthorized activity in one of our internal applications. We promptly engaged third-party experts to investigate and assist with remediation. Through that investigation, we determined that an unauthorized third party acquired data that potentially contained personal information. We then engaged a data-review firm to review the exfiltrated data. We received those results on August 30, 2024, and worked with counsel to determine which individuals to notify.

WHAT INFORMATION WAS INVOLVED?

The data accessed by the unauthorized person contained your personal information, including your name and Social Security number.

WHAT WE ARE DOING.

UMG takes the security of your personal information very seriously. We took immediate containment and mitigation actions upon detecting the unauthorized activity and worked with third-party experts, including outside counsel and a leading cybersecurity firm, to help us investigate the unauthorized activity and further secure our systems. Notice was not delayed as the result of a law enforcement investigation.

WHAT YOU CAN DO.

We encourage you to remain vigilant for any signs of unauthorized financial activity, and we are offering a complimentary 24-month membership to Experian’s IdentityWorks. Please review the next page for instructions on enrolling in IdentityWorks, as well as information on other steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION.

Should you have any questions or concerns, you can contact us at (888) 401-0393 on Monday through Friday 9:00 am - 7:00 pm Eastern Time, and one of our representatives will be happy to assist you. Thank you for your understanding.

Sincerely,

Saheli Datta
EVP, Chief Compliance Officer

MUSIC-ADT-CM

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary 24-month membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: 12/30/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** [REDACTED]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877)-208-8057 by **12/30/2024**, and provide them engagement number [REDACTED].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission (See contacts below.)

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland

Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York

Attorney General

The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

North Carolina

Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC

Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.