



August X, 2022

<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

NOTICE OF SECURITY INCIDENT

Dear _____,

We're writing to let you know about a potential breach of your personal information. We deeply regret that this has occurred, as keeping personal information safe and secure is very important to us and, as you will see below, we've taken robust steps to address the incident and protect your interests.

WHAT INFORMATION WAS INVOLVED?

The types of personal information that may have been accessed or obtained included your _____ . Targeted online monitoring has not revealed any indication that your personal information has been leaked.

WHAT WE ARE DOING

When we became aware of the incident, we quickly took steps to address it, including engaging outside cybersecurity experts to help remediate and ensure the ongoing security of our systems and began notifying the relevant authorities. As part of our ongoing efforts to ensure the security of our systems, we have enhanced cybersecurity protections throughout our environment and will continue to improve our security based on what we learn as appropriate.

We've hired Kroll, a global leader in risk mitigation and response, to provide you with credit and identity monitoring for two years, at no cost to you. You can find further information about these services, and how to sign-up, below.

Activation Code:

Expiration Date: October 6, 2022

Kroll Credit and Identity Monitoring

Key Features¹

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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

Enrollment Instructions

- Visit **[Enroll.krollmonitoring.com/redeem](https://enroll.krollmonitoring.com/redeem)** to activate and take advantage of your identity monitoring services.
- You have until **October 6, 2022** to activate your identity monitoring services.

¹ 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.

Activation Code:

Expiration Date: October 6, 2022
and Your Verification ID:

- Provide Your Activation Code:

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

WHAT YOU CAN DO

We strongly encourage you to take advantage of the Kroll credit and identity monitoring services we are providing to you free of charge. We also suggest that you remain vigilant about email links or attachments, and look out for any suspicious communications to your personal or business contact addresses, particularly those claiming to come from Warner Music Group or any Warner Music Group related websites.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained and any relevant government agency, such as IRS, SSA, or state DMV, as applicable.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, 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.

FOR MORE INFORMATION

Once again, we sincerely regret that this incident has occurred and have taken robust steps to address it. If you've any questions about the incident, please don't hesitate to contact us.

Sincerely,

Warner Music, Inc.

Activation Code:

Expiration Date: October 6, 2022

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.consumer.ftc.gov/features/feature-0014-identity-theft
1-877-IDTHEFT (438-4338)
1-866-653-4261 (TTY)

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:

equifax.com
www.equifax.com/CreditReportAssistance
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:

experian.com
www.experian.com/fraudalert
P.O. Box 4500
Allen, TX 75013
888-397-3742

TransUnion:

transunion.com
www.transunion.com/fraud
P.O. Box 2000
Chester, PA 19016
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 at least 90 days. 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 and obtain a copy of it.

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.
