October 8, 2021

BY ONLINE SUBMISSION

Office of the Attorney General
455 Golden Gate Ave.
St. 11000
San Francisco, CA

To Whom It May Concern:

On behalf of Terrier Media Buyer, Inc. dba Cox Media Group ("CMG" or the "Company"), and pursuant to Cal. Civ. § 1798.82(f), this letter provides notice of a cybersecurity incident involving California residents. By way of background, CMG is a for-profit broadcasting, publishing, and digital media services company operating in the United States, and its principal place of business is located at 1601 W Peachtree St. NE, Atlanta, Georgia 30309. Based on currently known information, CMG believes approximately 813 affected individuals reside in your jurisdiction.

On June 3, 2021, CMG experienced a ransomware incident in which a small percentage of servers in its network were encrypted by a malicious threat actor. CMG discovered the incident on the same day, when CMG observed that certain files were encrypted and inaccessible. CMG quickly took its systems offline as a precautionary measure and took additional steps to prevent further unauthorized access. CMG also began a thorough investigation with the support of leading outside cybersecurity experts and promptly reported the incident to the FBI, including the Newark and Dallas field offices. CMG did not pay a ransom or provide any funds to the threat actor as a result of this incident. There has been no observed malicious activity in CMG's environment since June 3, 2021.

Although there was no initial indication (including from the threat actor) that data may have been taken in the incident, and although none has been observed through continuous dark web monitoring by CMG, we recently determined that the threat actor tried to remove copies of certain HR files on a server, but the forensic evidence indicates that the attempt to do so may have been unsuccessful. To date, CMG has no evidence confirming that personally identifiable information was actually removed from CMG's systems or misused as a result of this incident. Nevertheless, CMG is notifying your office as well as individuals whose personal information was at risk of acquisition by the threat actor.

The types of personal information that were at risk of unauthorized acquisition included names, addresses, Social Security numbers, financial account numbers, health insurance information, health insurance policy numbers, medical condition information, medical diagnosis information, and online user credentials, stored for the purpose of human

resource management. CMG is not aware of any cases of identity theft, fraud, or financial losses to individuals stemming from this incident.

Soon after discovering the evidence the threat actor tried to remove copies of certain HR files, CMG began proactively informing known potentially affected individuals of the incident via email on July 30, 2021, and offered complimentary credit monitoring services to those individuals. Now that CMG has completed its document review process, CMG is sending notification letters to all individuals whose data the threat actor attempted to acquire and to provide complimentary credit monitoring services to this entire, identified population of individuals. CMG began providing notices on October 8, 2021 via U.S. Mail. Our detailed review of the population of affected individuals is ongoing, and we anticipate the possibility of additional notifications as we complete this process. We will provide your office with any material updates resulting from the investigation. The notice to individuals was not delayed as a result of a law enforcement investigation.

A sample notification letter has been included with our online submission. As previously mentioned and stated in the sample notice, CMG is offering to provide 24 months of free three-bureau identity theft and credit monitoring services through Experian.

Since discovering the incident, CMG has been working with the assistance of leading outside cybersecurity experts to enhance its security. The Company is continuing to monitor and improve its capabilities to detect any further threats and avoid any further unauthorized activity. These steps include multi-factor authentication protocols, performing an enterprise-wide password reset, deploying additional endpoint detection software, reimaging all end user devices, and rebuilding clean networks.

CMG takes the protection of personal information seriously and is committed to answering any questions that your office may have. Please do not hesitate to contact me at 470-446-1789 or Alysia.Long@cmg.com

Respectfully yours,

Alysia M. Long

Alysia Long
Vice President and Associate General Counsel
Cox Media Group

Enclosure

Sample Individual Notification Letter

October 8, 2021

[Full Name]
[Address 1]
[Address 2]
[City], [State] [Zip Code]

NOTICE OF DATA BREACH

Dear [FIRST NAME]:

We are writing to inform you of an incident potentially involving some of your personal information held by Terrier Media Buyer, Inc. dba Cox Media Group ("CMG"). We want to make clear at the outset that keeping personal data safe and secure is very important to us and we deeply regret that this incident occurred.

WHAT HAPPENED?

On or about June 3, 2021, a third party sought to disrupt our operations by means of an unauthorized, remote access to our computer network. After becoming aware of the incident, we quickly took steps to secure our systems and began a thorough investigation with the support of leading outside cybersecurity experts. We also promptly notified the FBI of the incident. CMG has determined that the unauthorized third party accessed a server containing limited personal information collected for human resources purposes. The unauthorized third party created a copy of that data on our systems and tried to remove a copy of that data from our network. We have completed our investigation and have no evidence confirming that your personal information was acquired by the unauthorized third party or misused as a result of this incident. Nevertheless, we are notifying you out of an abundance of caution because your information was contained in the data set that the unauthorized actor attempted to obtain.

WHAT INFORMATION WAS INVOLVED?

The types of personal information that the unauthorized third party may have obtained included your name, [additional data fields].

WHAT WE ARE DOING

We have implemented enhanced security controls and have been cooperating with law enforcement to investigate this incident.

October 8, 2021
Activation Code: _____
Expiration Date: December 31, 2021

Although at this time we have no indication of any misuse of your information, as a precaution, we are offering a complimentary two-year membership of IdentityWorksSM Credit 3B which includes credit monitoring and identity theft protection services through Experian.

Once you enroll, Experian provides you with the following key features:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

Enrollment Instructions

1. ENROLL by: December 31, 2021 (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/3bcredit
3. PROVIDE the **Activation Code:** [Activation Code]
    - Enrollment URL: https://www.experianidworks.com/3bcredit; Engagement number: [Engagement Number]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 281-4830**. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the identity restoration services by Experian.

Please refer to www.ExperianIDWorks.com/restoration for more information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at (833) 281-4830.

October 8, 2021
Activation Code: _____
Expiration Date: December 31, 2021

WHAT YOU CAN DO

We strongly encourage you to contact Experian and take advantage of the credit monitoring and identify theft protection services we are offering to you free of charge. Remain vigilant and carefully review your financial accounts for any suspicious activity.

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

FOR MORE INFORMATION

We take our responsibility to protect your information extremely seriously, and we sincerely regret any inconvenience this incident has caused you. If you have any questions, you can contact us at Inquiries@cmg.com or (833) 281-4830.

Cox Media Group

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

COX MEDIA 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 equifax.com/personal/credit-report-services P.O. Box 740241 Atlanta, GA 30374 866-349-5191	experian.com experian.com/help P.O. Box 2002 Allen, TX 75013 888-397-3742	transunion.com transunion.com/credit-help P.O. Box 1000 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 ability to place a security freeze on your credit report at no charge. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent but may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above and may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.

- The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

- To remove the security freeze, you must contact each of the three credit bureaus and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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 Colorado, Delaware, and Illinois residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

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 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. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

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 Georgia, 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 New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, http://www.ag.ny.gov/home.html, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, http://www.dos.ny.gov/consumerprotection, 1-800-697-1220.

For Rhode Island residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, http://www.riag.ri.gov/, (401) 274-4400.

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.