Walker Advertising, LLC
20101 Hamilton Avenue
Suite 375
Torrance, CA 90502

April 9, 2018

<<FIRST NAME>> <<LAST NAME>>
<<STREET ADDRESS>>
<<CITY>>, <<STATE>> <<ZIP CODE>>

Re: Notice of Data Breach

Dear **<<FIRST NAME>> <<LAST NAME>>**:

Walker Advertising, LLC ("Walker" or the "Company") is committed to safeguarding the personal information of its current and former employees as well as of these individuals' dependents which comes into the Company's possession. Unfortunately, I need to inform you of an information security incident that recently affected Walker and which may affect you because your personal information is in Walker's possession. I also want to tell you about the actions that Walker is taking to address this incident and to assure you that we have taken steps to prevent a recurrence.

What Happened?

Two senior Walker employees' corporate e-mail accounts were hacked between approximately January 29, 2018 and February 22, 2018. At least one of the corporate e-mail accounts was used to send phishing e-mails to solicit individuals to respond with access credentials to Walker's electronic information network. The employees who suffered the hacks reported the instances to Walker's Information Technology ("IT") Department. Upon learning of the hacks, the IT Department immediately isolated the affected e-mail accounts, stopped the phishing e-mails, and locked out the hacker. Walker reported the unlawful activity to the Federal Bureau of Investigation ("FBI") and will cooperate in any law enforcement investigation.

What Information Was Involved?

Promptly following the hack, Walker has undertaken a thorough investigation to determine what (if any) personal information was stored on the corporate e-mail accounts and/or entered in response to the phishing e-mails. The investigation determined either that (1) your personal information was stored in the affected individuals' corporate e-mail accounts due to the nature of their respective positions within the Company which necessitates access to this type of information; and/or (2) you entered your Walker user credentials in response to a phishing e-mail. The IT Department's investigation determined that potentially accessed information in the corporate e-mail accounts may include your name, Social Security number, driver's license number, medical information, and health insurance information. If you responded to a phishing

e-mail generated by a compromised e-mail account, your name, username, and password for your Walker online account was compromised.

What We Are Doing

First, we want to emphasize that we have no information indicating that any of your personal information has been misused. Walker notified the FBI about the incident to inform it of the unlawful activity which affected Walker's information security. Walker, however, has not delayed in notifying you as a result of any law enforcement agency's request.

Second, Walker promptly took steps to confirm whose information was potentially affected by the hacker's activities and to stem potential access to personal information. After locking out the hacker, Walker restored its information network security by requiring a change to all users' credentials with regard to accessing our system. Further, to limit access to personal information, we enabled a multi-factor authentication tool for individuals with access to this type of information.

Third, out of an abundance of caution, Walker is offering you one year of identity protection services at no cost to you through Experian, one of the three nationwide credit bureaus. Your free, one-year membership in Experian's IdentityWorks^{SM} product provides identity restoration services, fraud detection tools, and other benefits which include monitoring your credit file. Starting today, if you suspect that your personal information has been used fraudulently, you can call Experian's identity restoration agents to assist you to investigate and resolve any incidents of fraud. You may take advantage of this benefit, at any time, until March 28, 2019, by calling Experian at 877-890-9332. No enrollment or activation is necessary. The terms and conditions for identity restoration are located at www.ExperianIDWorks.com/restoration.

While identity restoration is immediately available to you, we also encourage you to activate fraud detection tools available through IdentityWorks^{SM}. This product provides you with superior identity detection, credit monitoring, and resolution of identity theft.

If you wish to enroll in IdentityWorks^{SM}, you will need to do the following:

1. **Visit** the IdentityWorks^{SM} web site: https://www.experianidworks.com/credit

or call 1-877-890-9332 to enroll and provide Engagement Number DB06115

2. **PROVIDE** your Activation Code: [CODE]

Enrollment Deadline: June 30, 2018 (your Activation Code will not work after this date)

If you have any questions concerning IdentityWorks^{SM} or if you prefer to enroll over the phone for delivery of your membership via US mail, please call Experian at 1-877-890-9332. Be prepared to provide Engagement Number DB06115 as proof of eligibility for the identity protection product by Experian.

What You Can Do

In addition to the steps Walker has taken to provide you with identity protection services, we have included with this letter additional information on steps you can take to protect the security of your personal information. We urge you to review this information carefully.

Other Important Information

To help prevent a recurrence of this data security incident, Walker is conducting a thorough review of its current policies and procedures. Based on that review, we will evaluate what additional steps are needed to enhance the strong protections we already have in place for safeguarding personal information.

For More Information

Walker sincerely regrets any inconvenience this incident may cause you. If you have any questions, please call us at 310-519-4050 between 09:00 AM and 5:00 PM (Pacific Time), Monday through Friday (excluding holidays). When you call, please inform the operator that you are calling regarding the information security incident and ask for Jean Delago.

Sincerely,

Quentin Kluthe
Chief Financial Officer

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in IdentityWorks℠. You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IdentityWorks℠ membership. If you need assistance or if you want to enroll by telephone, you should contact Experian directly at 1-877-890-9332. Experian's IdentityWorks℠ product will provide the following:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring**: Actively monitors your Experian credit file for indicators of fraud.
- **Identity Restoration**: Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks℠ ExtendCARE**: You will receive the same high level of identity restoration support even after your IdentityWorks℠ membership has expired.
- **$1 Million Identity Theft Insurance**[2]: Provides coverage for certain costs and unauthorized electronic fund transfers.

Please direct questions about the IdentityWorks℠ product to Experian. A credit card is not required for enrollment in IdentityWorks℠. Enrollment in IdentityWorks℠ will not affect your credit score.

2. Review your credit reports. You can receive free credit reports by placing a fraud alert. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

3. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other service providers.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from Experian, contact an IdentityWorks℠ identity resolution agent toll-free at **1-877-890-9332** or visit www.ExperianIDWorks.com/restoration for additional information. You should consider changing your username, passwords, security questions, and security answers to your online accounts. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You should also consider reporting such activity to your local police department, your state's attorney general, and the Federal Trade Commission.

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

5. Consider placing a fraud alert with one of the three national credit bureaus. You can place an initial fraud alert by contacting one of the three national credit bureaus listed below. For 90 days, an initial fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. You can also obtain information from the three national credit bureaus about placing a security freeze to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. There may be a cost associated with placing a security freeze.

The contact information for all three bureaus is as follows:

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

6. Additional Information. You can obtain additional information about steps you can take to avoid identity theft from the following:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.ftc.gov/idtheft/
(877) IDTHEFT (438-4338)
(202) 326-2222

Firmwide:153764016.2 999999.0654