WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

May 31, 2013

Lori Nugent
312.821.6177 (direct)
Lori.Nugent@wilsonelser.com

Attorney General Michael Delaney
Office of the Attorney General
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Delaney:

We represent Primedia, Inc., now known as RentPath, Inc. ("Primedia"), with respect to a security incident involving the potential exposure of certain personal information described in detail below. Primedia is a digital advertising company that provides consumers with listings and other information regarding apartments and homes for rent.

Primedia takes the security of the information in its control very seriously. Accordingly, it has taken steps to identify individuals whose sensitive data may have been exposed in the incident discussed below, and provide appropriate services to them including continuous credit monitoring and enhanced identity theft consultation and restoration. At present there is no indication that the information has been inappropriately accessed, misused or further disclosed. Primedia also has taken steps to prevent this type of incident from occurring in the future. The following paragraphs provide further detail about this incident.

1. Overview of breach

On June 20, 2012, an independent contractor working in Primedia's network operations group was observed on security tapes stealing several pieces of computer hardware from Primedia's headquarters. Subsequently, it was determined that a backup storage device that was stolen held personally identifiable information ("PII") of employees, former employees and applicants, stored within 4.8 terabytes of data. No PII was on the other devices.

It has been difficult to recover, extract and analyze the data that was contained on the stolen device. Considerable time was required to attempt to recover the data from 31 backup tapes. Ultimately, FishNet Security ("FishNet") was retained to recover the data and to assist in determining whether PII was included in the data on the stolen device.

Months of analysis by FishNet Security ("FishNet") have been necessary to determine whether the data may have contained PII. Ultimately, FishNet identified over 800,000 file pathways where PII may have been located. Manual review of the 800,000 file pathways identified approximately 56,000 social security numbers that were contained in the data on the stolen device. Primedia was able match social security numbers that were on the stolen device to

names and addresses of approximately 30,000 employees, former employees and applicants by reconciling the social security numbers with its internal human resources system. Notification of these individuals has commenced, and credit monitoring and optional identity restoration services through Kroll Advisory Solutions ("Kroll") are being offered at no cost to the impacted individuals.

For the remaining approximately 26,000 social security numbers that were found in the data on the stolen device, notification cannot be made until sufficient contact information is located. Kroll is working forensically with the available data to identify names associated with the approximately 26,000 social security numbers. Once names are obtained, Kroll will utilize its address Locator service to obtain the most recent address for these individuals so they can be notified.

The identification of contact information for impacted individuals also has been difficult, because of the manner in which the data was stored. The difficulty that Primedia and its vendors have experienced in locating PII and matching social security numbers to names and addresses of individuals would similarly be experienced if someone were to attempt to misuse the data on the stolen device.

If it would be useful, we are happy to further discuss the work that has been necessary to extract PII and identify impacted individuals, as well as the notification and services that are being provided to the individuals for whom address information has been obtained, and the steps that are being taken to obtain address information for the remaining individuals. For your convenience, a summary timeline of events is provided as follows:

- June 20, 2012 – An independent contractor working in Primedia's network operations group was observed on security tapes stealing several pieces of computer hardware from Primedia's headquarters. The contractor is terminated and Primedia's Internal Audit Department commences an investigation.

  June 25, 2012 – Primedia's Internal Audit Department delivers its preliminary report to the Company's General Counsel, and a police report is filed with the Gwinnett County Police Department.

- June 21, 2012 – August 31, 2012 – Primedia conducts an internal investigation, including reviewing security tapes, card access records, the independent contractor's computer logs, and conducting an inventory of equipment. From the investigation, Primedia learns, among other things, that: 1) the independent contractor had searched the internet to investigate how to delete data contained on storage devices; 2) a storage device containing 4.8 terabytes of data was stolen which may contain sensitive information; and 3) backup tapes of the storage device were available. The information on the storage device was contained on thirty-one (31) backup tapes.

- August 15, 2012 – October 2012 – Primedia begins the process of determining what data was stored on the stolen device. Primedia obtains the backup tapes from its secure offsite vault at Iron Mountain. Simultaneously, Primedia also acquires and

configures a new storage array to house the backup tapes. With the new storage array in place, Primedia attempts to recover the data several times, using different restoration techniques and hardware to recover the data. Unfortunately, recovery is not successful, as each attempt results in the corruption of the resulting data catalog, rendering the restore unusable. Based on its inability to restore the data, Primedia begins researching vendors that specialize in forensic recovery with the goal of retaining a vendor to recover the data.

- October 11, 2012 – The independent contractor, who was caught on security tapes stealing the hardware, was arrested but continues to deny any allegations of theft. Primedia subsequently has confirmed that the arrested individual attempted to sell what appeared to be the stolen equipment to a number of resellers. This fact, along with the fact that the thief had performed online research regarding methods for wiping storage devices clean, leads the Company to believe that the apparent goal of the arrested individual was to sell the hardware for quick cash, and that he was not a hacker interested in the information contained on the devices.

- November 2, 2012 – FishNet Security ("FishNet") is hired to recover the data on the backup tapes.

- November 2, 2012 – December 20, 2012 – FishNet obtains the backup tapes and ultimately recovers the information on the tapes. During this process, FishNet also successfully creates a catalogue for the data on the device.

- December 20, 2012 – FishNet provides Primedia with a copy of the recovered data. Primedia reviews the data, and determines that the device contained the network libraries for various corporate departments; it is not yet apparent that any PII is on the device. Primedia then engages FishNet to conduct an e-discovery type search for social security numbers, credit card numbers, and bank account information to determine whether any personally identifiable information was on the device.

- January 2, 2013 – March 20, 2013 – Search terms are developed, and FishNet begins its analysis of the recovered data. Because of the amount of information, FishNet is only able to identify the file pathways where personally identifiable information may be contained. FishNet identifies over 800,000 file pathways. FishNet is not able to identify the specific documents, rule out all false positives, or determine whether names are collocated with social security numbers or other limited financial information.

- March 20, 2013 – May 9, 2013 – Primedia begins manually analyzing the identified file pathways. This analysis requires Primedia to navigate to each of the 800,000 file pathways separately, view documents to determine whether the document contained PII, and create a spreadsheet into which Primedia manually input any social security numbers that were found on any document reviewed. Approximately 56,000 social security numbers are found. Of the 56,000 social security numbers, Primedia obtains the names and address for approximately 30,000 individuals by reconciling the social

security number with Primedia's human resources system. Primedia updates the spreadsheet manually with each individual's name and address. For the remaining 26,000 records, Primedia determines that the names and addresses of these individuals are embedded in multiple documents and data fields that would be extremely time consuming to locate and extract.

- April 30, 2013 – Primedia engages Kroll Advisory Solutions ("Kroll") to provide breach response services, including sending the notification letters to the impacted population, providing call center services, and providing credit monitoring and enhanced identity theft consultation and restoration.

- May 20, 2012 – Kroll informs Primedia that it requires the name ***and*** social security number to obtain the latest address using its Locator database. Primedia has only the social security number for the remaining 26,000 individuals.

- May 20, 2013 – Primedia engages Kroll to conduct an analysis for the remaining 26,000 social security numbers in order to extract the name and social security number of the individuals into a spreadsheet that will then be reconciled against Kroll's Locator service to obtain the most recent addresses.

- May 23, 2013 – Notification letters are issued to the first 30,000 individuals for whom name and address has been identified.

- May 28, 2013 – Kroll begins its analysis on the remaining 26,000 files to connect the social security number and name of these individuals.

Once Kroll completes its analysis and extracts the name and social security number from the files for the remaining 26,000 potentially impacted individuals, it will then reconcile this information against its address Locator service to obtain the most recent mailing addresses. We plan to mail notification letters to the remaining 26,000 potentially impacted individuals as soon as practicable, with the goal of mailing the letters within seven days of the date when Kroll provides its completed analysis to Primedia. At that time, Kroll also will provide Primedia with an analysis of the number of individuals affected by state.

2. Number of New Hampshire residents affected

The initial mailing provided notice to 75 New Hampshire residents who were affected by the theft of the storage device. A copy of the notification letter is included with this letter.

Once Kroll completes its analysis of the remaining 26,000 potentially impacted individuals, we will provide an updated notification communication specifying the additional number of New Hampshire residents, if any, who were affected by the theft of the storage device. We also will provide a copy of the notification sent to those individuals.

3. Steps taken or planned relating to the incident

Primedia has taken several steps to prevent this type of event from happening again, including increasing the security of its data storage devices, encrypting data, increasing physical security at its facilities, updating its data retention policies, and reviewing and updating its procedures for hiring independent contractors to incorporate additional security checks.

Because social security numbers were included on the storage device, Primedia is providing individuals whose information was on the stolen device with continuous credit monitoring and enhanced identity theft consultation and restoration services through Kroll. At present there is no indication that the information has been inappropriately accessed, misused or further disclosed.

4. Other notification and contact information

Notification has been provided to the Consumer Reporting Agencies.

* * *

Primedia takes the security and privacy of the information in its control very seriously, and has taken steps to prevent this type of incident from occurring in the future. Should you have any questions or concerns, or require additional information, please do not hesitate to contact me.

Very truly yours,

WILSON, ELSER, MOSKOWITZ, EDELMAN & DICKER LLP

Lori S. Nugent

Lori S. Nugent

cc: Melissa K. Ventrone, Wilson Elser

PRIMEDIA®

<<Firstname>> <<Middlename>> <<Lastname>>
<<Address1>>
<<Address2>>
<<City>>, <<Stateprovince>> <<Postalcode>>
<<Intelligent Mail Barcode>>

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

Dear <<Firstname>> <<Middlename>> <<Lastname>>,

We recently discovered a security incident that occurred at our offices which may have resulted in the exposure of some of your personal information. At this time, we are not aware of any misuse of your personal information. We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this may cause you.

We recently experienced the theft of over fifty pieces of computer hardware from our facilities. Upon investigating this event, we learned that three computer storage devices were among those stolen. Although the devices were not encrypted, they were password protected. At that time, we attempted to discover what information was on the devices by restoring the backup tapes. Unfortunately, the backup tapes were corrupted. We then retained an expert company specializing in computer forensics, which successfully restored the tapes and then conducted an analysis on the data. On March 6, 2013, following forensic analysis, we learned that one of the devices contained your name, Social Security number, and may have contained limited financial information.

We believe that the goal of the perpetrator was to sell the hardware for quick cash. We do not believe he was interested in the data contained on the devices. The person responsible has been identified and arrested. We want to make you aware of this situation even though we believe it is unlikely that your information has been or will be misused.

We have also taken measures to prevent this type of event from happening again, including updating our data retention policies, increasing the security of our data storage devices, including the use of encryption technology, and increasing physical security at our facilities.

As stated above, we are not aware of any misuse of your information. However, out of an abundance of caution, we have engaged the services of Kroll Advisory Solutions to provide identity theft safeguards at no cost to you through its iDTheftSmart™ program. Kroll Advisory Solutions is a global leader in risk mitigation and response, and their team has extensive experience helping people who have experienced this type of event.

Next Steps

Your membership number is: <<MEMBERSHIPNUMBER>>

1. **Go to www.idintegrity.com to start your credit monitoring**
   Please be prepared to provide your membership number. Instructions are provided online.

   If you would prefer to receive your alerts through the mail instead of online, fill out the enclosed *Consumer Credit Report and Credit Monitoring Authorization Form* and return it in the enclosed postage-paid envelope.

2. **Call 1-???-???-???? if you need help or have questions**
   8 a.m. to 5 p.m. (Central Time), Monday through Friday
   Kroll representatives are ready to help you.

9xxxxxxx-xxxx

We are providing you with access to **Continuous Credit Monitoring** and **Enhanced Identity Theft Consultation and Restoration** from Kroll Advisory Solutions at no cost to you. Please note that in order to activate these services you will need to follow the instructions in the "Next Steps" box on the first page of this letter.

Continuous Credit Monitoring. We are providing you with no-cost access to Kroll's credit monitoring service for 12 months from the date of this letter. Once activated, you will receive alerts whenever there are certain changes in your credit file that could indicate an issue.

Enhanced Identity Theft Consultation and Restoration. Kroll's Licensed Investigators are available to listen, to answer your questions and offer their expert advice regarding any concerns you may have. And in the unlikely event that your name or credit is affected by this incident, your investigator will do most of the work necessary to restore your identity on your behalf.

To receive credit monitoring, 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.

We sincerely regret any inconvenience or concern that this matter may have caused you. If you have any questions or concerns regarding this incident, please call (???) ???-???? Monday through Friday from 8 a.m. to 5 p.m. (Central Time). Kroll's Licensed Investigators are standing by to answer your questions or help you with concerns you may have. *Please have your membership number ready.*

Sincerely,

Charles J. Stubbs
President and Chief Executive Officer,
Primedia, Inc. n/k/a RentPath, Inc.

State Notification Requirements

All States.
More information can also be obtained about protecting your identity by contacting the Federal Trade Commission listed below.

You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, Georgia 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

For residents of Iowa.
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon.
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Illinois, Maryland and North Carolina.
You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about steps you can take toward preventing identity theft.

Maryland Office of the Attorney General	**North Carolina Office of the Attorney General**	**Federal Trade Commission Consumer Response Center**
Consumer Protection Division	Consumer Protection Division	600 Pennsylvania Avenue, NW
200 St. Paul Place	9001 Mail Service Center	Washington, DC 20580
Baltimore, MD 21202	Raleigh, NC 27699-9001	1-877-IDTHEFT (438-4338)
1-888-743-0023	1-877-566-7226	www.ftc.gov/bcp/edu/microsites/idtheft/
www.oag.state.md.us	www.ncdoj.com	

For residents of Massachusetts.
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts and West Virginia.
You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at the top of this page. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.