



11/4/2011

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

Dear Attorney General Delaney:

Pursuant to New Hampshire law, we are writing to notify you of unauthorized access or use of personal information involving 13 New Hampshire residents.

#### **Nature of the Unauthorized Access or Use of Personal Information**

On October 24<sup>th</sup>, 2011, a former Monster Worldwide, Inc. ("Monster") employee notified Monster's Human Resources department that she conducted a Google search on her name and, on the second page of results, found a link to spreadsheet that contained her name, address, date of birth, social security number, and salary information. Upon investigation, Monster discovered the spreadsheet was stored in a file directory on the personal website of another former Monster employee. The spreadsheet appears to have been created in March 2003, but it is unknown when this information first appeared online. It contained the following information of certain former Monster employees:

- Name
- Job title
- Social Security Number
- Address
- Birth date
- Salary
- Termination date

Monster has no evidence of any adverse impact to the former employees involved. However, Monster recognizes the possibility that the information may have been accessed during the period it was available online.

Under current Monster policy and practice, access to this type of information is highly restricted and the data is only stored in encrypted format and systems. As this event likely occurred in excess of eight years ago, it is difficult to assess the cause of the incident, but we are very confident in saying that a similar occurrence would be extremely unlikely to occur now.

#### **Number of New Hampshire Residents Affected**

The spreadsheet included personal information of 13 residents of New Hampshire. These residents have received or will shortly receive written notice pursuant to New Hampshire law. Notice will be sent via post to the address listed on the spreadsheet. A copy of this notice is included as an attachment to this letter.

#### **Steps Monster Has Taken and Plans to Take Relating to the Incident**

Upon discovery of the spreadsheet, Monster immediately alerted its security team for investigation. Internal investigation confirmed the breach, and Monster's executive team was notified, including the General Counsel and the Chief Privacy Officer.

Monster promptly contacted the website owner to have the content removed, which he did immediately after receiving Monster's request. The owner stated that he did not intend to have the file or to make it public. He did not remember why he had the file and did not realize the directory and its contents were publicly available or that they had been indexed by Google. The owner, a former Monster employee, had left the company in 2007.

At Monster's request, Google removed its cached copy of the spreadsheet and by October 25th it was no longer appearing in Google search results. Monster's investigation determined that the file did not appear in search results for other major search engines, including Bing, Yahoo, AOL, and Ask. Monster has notified the former employee who reported the incident that the file has been removed and that her information is no longer available.

Monster is in the process of notifying New Hampshire residents affected by the incident. Monster will provide these individuals with a year of credit monitoring and identity theft protection.

Law enforcement has not been engaged in this matter. Monster does not believe there was any malicious intent behind the incident. The directory containing the spreadsheet also contained personal documents of the site owner, which were not intended to be publicly available. Further, Monster has not received any reports or complaints of identity theft from affected individuals.

Monster takes its obligation to protect employee data very seriously. We have made significant enhancements to our security posture over the last several years and feel confident that this type of incident would not occur today given our current policy and practice. Additionally, Monster provides employees with annual training on how to handle and protect personal information. Should you have additional questions or require anything further, please do not hesitate to contact Gretchen Herault, Vice President and Deputy Chief Privacy Officer at:

[gretchen.herault@monster.com](mailto:gretchen.herault@monster.com)

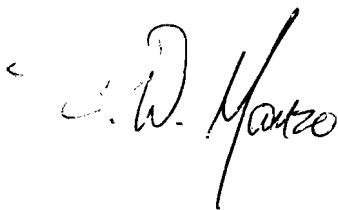
978-823-2209

5 Clock Tower Place

Suite 500

Maynard, MA 01754

Sincerely,



Patrick W. Manzo  
Executive Vice President  
Monster Worldwide, Inc.



[Date]

[First Name] [Last Name]

[Resident Address Line 1]

[Resident Address Line 2]

[City, State ZIP]

Dear [First Name]:

We are writing to notify you of a security incident involving your personal information. On October 24, 2011, Monster discovered a file stored on the personal website of a former employee that contained the personal information of certain former Monster employees. The spreadsheet contained the following information about you:

- Name
- Job title
- Social Security Number
- Address
- Birth date
- Salary
- Termination date from Monster

The spreadsheet was not publicized anywhere on the web and could only be found through a specific Google search. Although Monster has no evidence of any adverse impact to affected individuals, it is possible that your personal information may have been potentially exposed to others.

Upon discovery the file was removed from the former employee's website and cached copies were removed from search results. It is no longer available.

### **Identity Theft Protection and Credit Monitoring**

We are sorry that this information was available online and we apologize for any inconvenience this has caused you.

To help protect your identity, we are offering a complimentary one year membership of Experian's ProtectMyID™ Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft.

### **Activate ProtectMyID Now in Three Easy Steps**

1. ENSURE that you enroll by: February 29, 2012

2. VISIT the ProtectMyID website: [www.protectmyid.com/enroll](http://www.protectmyid.com/enroll) or call 877-371-7902 to enroll
3. PROVIDE your activation code:

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You will receive timely Credit Alerts from ProtectMyID on any key changes in your credit report which could include new inquiries, new credit accounts, medical collections and changes to public records.

ProtectMyID provides you with powerful identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service.

**Your complimentary 12-month ProtectMyID membership includes:**

- **Credit Report:** A free copy of your Experian credit report
- **Daily Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections
- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated agent who will walk you through the fraud resolution process from start to finish
- **\$1 Million Identity Theft Insurance\*:** As a ProtectMyID member, you are immediately covered by a \$1 million insurance policy that can help you cover certain costs including lost wages, private investigator fees, and unauthorized electronic fund transfers.

**Activate your membership today at [www.protectmyid.com/enroll](http://www.protectmyid.com/enroll) or call 877-371-7902 to register with the activation code above.**

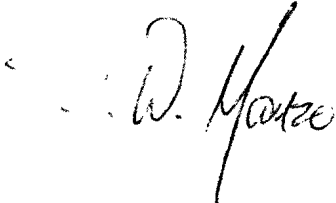
Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902. We sincerely apologize for this incident and encourage you to take advantage of the identity theft protection service.

We take our obligation to protect employee data very seriously. We have made significant enhancements to our security posture over the last several years and feel confident that this type of incident would not occur today given our current policy and practice. Additionally, Monster provides employees with annual training on how to handle and protect personal information. Should you have any questions or concerns regarding this matter or the protections available to you, please do not hesitate to contact Gretchen Herault, Vice President and Deputy Chief Privacy Officer at:

[gretchen.herault@monster.com](mailto:gretchen.herault@monster.com)

978-823-2209  
5 Clock Tower Place  
Suite 500  
Maynard, MA 01754

Sincerely,

A handwritten signature in black ink, appearing to read "P. W. Manzo". The signature is written in a cursive style with a large, stylized initial "P".

Patrick W. Manzo  
Executive Vice President  
Monster Worldwide, Inc.

\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. 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.