



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

March 6, 2008

Timothy C. Blank
Dechert, LLP
200 Clarendon Street
27th Floor
Boston, MA 02116-5021

Re: Monster Worldwide, Inc.

Dear Mr. Blank:

As you know, the Division of Privacy and Identity Protection staff has been investigating possible violations of Section 5 of the Federal Trade Commission Act by your client, Monster Worldwide, Inc. (“Monster”). According to August, 2007, news reports, unauthorized individuals obtained personal information – including names, phone numbers, and email addresses – of over a million consumers who sought jobs using Monster’s services; the individuals then apparently used that personal information to engage in targeted phishing campaigns, sending personalized emails to Monster customers purportedly on behalf of Monster.¹

Targeted phishing campaigns are a growing concern as they tend to be more successful than traditional phishing schemes. At least one study has concluded that targeted phishing campaigns result in a far higher percentage of recipients “taking the bait” than non-targeted phishing campaigns.² We are concerned that the availability of large numbers of email addresses and other customer contact information from a single commercial entity may help facilitate these targeted phishing attacks.

Our investigation of Monster sought to determine whether Monster engaged in unfair or deceptive acts or practices by failing to provide reasonable security for its customer contact information. The investigation focused on the risks raised by Monster’s storage of this information and whether Monster acted reasonably in anticipating and addressing those risks. As you know, the staff identified a number of concerns regarding the timing of Monster’s implementation of enhanced security measures to prevent unauthorized access to customer contact information.

Despite these concerns, the staff has determined to close the investigation. Among the

¹ Among other things, the emails encouraged recipients to click on an embedded link which likely installed malware, such as a keystroke logger, useful in obtaining sensitive customer data, including financial account log-in credentials.

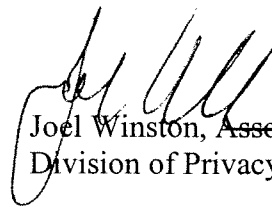
² See, e.g., G. Kaizer, *FAQ, The Monster.com Mess* (Aug. 24, 2007), Computerworld, available at <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032518>.

factors we considered were the extent to which the risk at issue was reasonably foreseeable at the time of the compromise; the nature and magnitude of the risk relative to other risks; the benefits relative to the costs of protecting against the risk; Monster's overall data security practices; the duration and scope of the compromise; the level of consumer injury; the type of information disclosed without authorization; and Monster's overall response to the incident. Applying these factors, the circumstances in this matter contrast with those in recent enforcement actions brought by the Commission, many of which involved significant failures to address well-known vulnerabilities affecting inherently sensitive personal information such as Social Security numbers and credit card numbers.

We continue to emphasize that data security is an ongoing process, and that as risks, technologies, and circumstances change over time, companies must adjust their information security programs accordingly. As noted above, the staff is concerned with the growing prevalence of personalized or targeted phishing attacks – attacks that may be facilitated by the failure to provide reasonable security for storehouses of customer contact information accessible for viewing and downloading online. Thus, we expect companies that house such data to take appropriate steps to protect it. Depending on the circumstances, such steps may include: avoiding the use of simple, easily guessed passwords or other credentials used by customers to access company data; implementing measures to ensure that those who access the company's online services using legitimate customer credentials are in fact authorized users of the system; and training customer service representatives to detect and defeat attempts to obtain customer credentials through social engineering or pretexting. We also support efforts by companies to educate customers regarding the threats posed by individuals obtaining customer contact information for use in targeted phishing attacks. Further, we expect such companies to remain vigilant in identifying new methods of attack by fraudsters and identity thieves and taking reasonable precautions to defend against such attacks.

The closing of this investigation is not to be construed as a determination that a violation may not have occurred, just as the pendency of an investigation should not be construed as a determination that a violation has occurred. The Commission reserves the right to take such further action as the public interest may require.

Sincerely,



Joel Winston, Associate Director
Division of Privacy and Identity Protection