122 3095

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	
GMR TRANSCRIPTION SERVICES, INC., a corporation,	)	
AJAY PRASAD	)	**DOCKET NO. C-**
and	)	
SHREEKANT SRIVASTAVA, individually and as officers of GMR Transcription Services, Inc.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that GMR Transcription Services, Inc., Ajay Prasad, and Shreekant Srivastava have violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. GMR Transcription Services, Inc. ("GMR"), is a California corporation with its principal office at 2512 Chambers Road, Suite 206, Tustin, CA 92780.

2. Respondent Ajay Prasad is president of respondent GMR and owns 80% of the company. He has authority to control the conduct of respondent GMR. Individually or in concert with others he formulates, directs, or controls the policies, acts, or practices of respondent GMR, including the acts or practices alleged in this complaint. His principal office or place of business is the same as respondent GMR.

3. Respondent Shreekant Srivastava is vice president of respondent GMR and owns 20% of the company. He has authority to control the conduct of respondent GMR. Individually or in concert with others he formulates, directs, or controls the policies, acts, or practices of respondent GMR, including the acts or practices alleged in this complaint. His principal office or place of business is the same as respondent GMR.

4. The acts and practices of respondents alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

5. At all relevant times, respondents have been in the business of transcribing digital audio files ("audio files") for individuals and businesses in a variety of professions and industries. Respondents' customers include: university students and faculty; well-known corporations (including retailers, insurers, and telecom and financial service providers); government agencies; and health care providers and hospitals.

6. Respondents conduct their transcription business almost entirely online using: respondents' own computers and devices; various websites; and computers and devices leased from third-party service providers that are operated by or for respondents (collectively, "respondents' computer network").

7. In conducting business, respondents rely almost exclusively on independent service providers to transcribe audio files that respondents assign to them. Respondents:

   (a) assign non-medical audio file transcriptions to at least 100 independent typists located in North America; and

   (b) automatically assigned all medical audio file transcriptions to Fedtrans Transcription Services, Inc. ("Fedtrans"), between at least January 1, 2009, and May 1, 2012. Fedtrans, which is located in India, assigned respondents' files to independent typists to transcribe.

8. At all relevant times, respondents' transcription process began when a customer logged in to one of respondents' websites and uploaded an audio file to a leased server located on respondents' computer network. Based on the type of file, respondents assigned the audio file to one of their independent typists or Fedtrans. After being notified of the assignment, the typist or Fedtrans logged in to the website and downloaded the file. Fedtrans followed a similar process through which an independent typist downloaded the file from Fedtrans' computer network. After downloading it, the typist converted the audio file into a Microsoft Word file ("transcript file") and then followed the reverse process to upload it back to respondents' computer network. Afterwards, respondents either emailed the transcript file to the customer or notified the customer to retrieve the file from respondents' computer network.

9. Audio files and transcript files can include sensitive information from or about consumers, including children. This information can include, but is not limited to: names, dates of birth, addresses, email addresses, telephone numbers, Social Security numbers, driver's license numbers, tax information, medical histories, health care providers' examination notes, medications, and psychiatric notes (collectively, "personal information").

10. Since at least 2006, respondents have disseminated or caused to be disseminated privacy policies and statements, including, but not necessarily limited to, the following statements regarding the privacy and security of personal information:

- Why GMR Transcription Services? . . . Security Measures to Protect Your Confidentiality.

- Each transcriptionist within the GMR community is required to sign a Confidentiality Agreement prior to working for us. This is kept on file. You can be assured that the materials going through our system are highly secure and are never divulged to anyone.

(**Exhibit A**: www.gmrtranscription.com (from 2006 through 2013)).

- HIPAA Compliant Medical Transcription Service

(**Exhibit B:** www.gmrmedicaltranscription.com (from 2006 through May 2012)).

- It is often asked what one needs to be careful while choosing an outsourcing transcription company. In the medical industry, security and privacy are extremely important. In outsourcing arrangements with services and healthcare vendors, you can check the vendor's expertise and credibility by HIPAA compliance. Amongst all the rules that are stipulated by HIPAA, ones concerned with security, health care compliance and privacy are deemed to be important by outsourcing experts. The benefits include giving greater accuracy, data security, and absolute privacy for all of their patient's (sic) records and documents. Look for a company that is HIPAA compliant and takes proper measures to ensure security, health care compliance and privacy. A good company will make sure that the sensitive information related to patients is handled with great care. From compliance training and secure systems to the confidentiality agreements, Transcription Companies cover all the aspects involved in the HIPAA regulations.

(**Exhibit C:** GMR Blog, http://blog.gmrtranscription.com/securing-medical-transcription-data-with-hipaa/ (posted Feb. 23, 2010 through present).

- HIPAA compliant medical transcription is the basic need of any medical professionals and hospitals.

(**Exhibit D:** Twitter (Sept. 19, 2010) @gmrtranscript).

11. Respondents have engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to protect personal information in audio and transcript files. Among other things, respondents failed to:

(a) require typists to adopt and implement security measures, such as installing anti-virus applications, or confirm that they had done so;

(b) adequately verify that their service provider, Fedtrans, implemented reasonable and appropriate security measures to protect personal information in audio and transcript files on Fedtrans' network and computers used by Fedtrans' typists. For example, respondents did not:

(1) require Fedtrans by contract to adopt and implement appropriate security measures to protect personal information in medical audio and transcript files, such as by requiring that files be securely stored and securely transmitted to typists (e.g., through encryption) and authenticating typists (e.g., through unique user credentials) before granting them access to such files; and

(2) take adequate measures to monitor and assess whether Fedtrans employed measures to appropriately protect personal information under the circumstances. Respondents did not request or review relevant information about Fedtrans' security practices, such as, for example, Fedtrans' written information security program or audits or assessments Fedtrans may have had of its computer network.

12. As a result of these security failures, respondents were unaware that Fedtrans used a File Transfer Protocol ("FTP") application to both store medical audio and transcript files on its computer network and transmit the files between the network and its typists. The application stored and transmitted files in clear readable text and was configured so that the files could be accessed online by anyone without authentication. A major search engine therefore was able to reach the Fedtrans FTP application and index thousands of medical transcript files that respondents had assigned to Fedtrans (collectively, the "Fedtrans files"). The files were publicly available, and were accessed, using the search engine.

13. The Fedtrans files were prepared between March 2011 and October 2011. They included personal information, such as names, dates of birth, health care provider names, examination notes, medical histories, medications, and, in some cases, employment histories and marital status. Some of the files contained children's examination notes and highly sensitive medical information, such as information about psychiatric disorders, alcohol use, drug abuse, and pregnancy loss. Such information can easily be misused to cause substantial consumer injury, such as identity theft, and unauthorized access can cause harm by disclosing sensitive private medical information.

14. Respondents could have corrected their security failures using readily available, low-cost security measures.

15. Consumers have no way of independently knowing about respondents' security failures and could not reasonably avoid possible harms from such failures.

16. After being informed that the Fedtrans files were available online in clear readable text, respondents notified Fedtrans and asked the search engine that had indexed the files to remove the files from its cache.

VIOLATIONS OF THE FTC ACT

COUNT I

17. Through the means described in Paragraph 10, respondents represented, expressly or by implication, that they implemented reasonable and appropriate security measures to prevent unauthorized access to the personal information in audio and transcript files.

18. In truth and in fact, as described in Paragraphs 11-14, respondents did not implement reasonable and appropriate security measures to prevent unauthorized access to personal information in audio and transcript files. Therefore, the representation set forth in Paragraph 17 was false or misleading and constitutes a deceptive act or practice.

COUNT II

19. Through the means described in Paragraph 10, respondents represented, expressly or by implication, that they took reasonable measures to oversee their service providers to ensure such service provider implemented reasonable and appropriate security measures.

20. In truth and in fact, as described in Paragraphs 11-14, respondents did not take reasonable measures to oversee their service providers to oversee ensure such service providers implemented reasonable and appropriate security measures. Therefore, the representation set forth in Paragraph 19 was false or misleading and constitutes a deceptive act or practice.

COUNT III

21. As set forth in Paragraphs 11-15, respondents failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information in audio and transcript files. Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

22. The acts and practices of respondents as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this _____ day of _____ , 2014, has issued this complaint against respondents.

By the Commission.

Donald S. Clark
Secretary