Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekant Srivastava,
File No. 122 3095

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from GMR Transcription Services, Inc. ("GMR"), Ajay Prasad ("Prasad"), and Shreekant Srivastava ("Srivastava") (taken together, "respondents")

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Respondents are in the business of transcribing digital audio files for individuals and businesses in a variety of professions and industries. Respondents conduct their transcription business almost entirely online, where customers can upload audio files for transcription. Respondents rely almost exclusively on independent service providers to transcribe audio files that respondents assign to them. Respondents assign non-medical audio file transcriptions to at least 100 independent typists located in North America, and, between at least January 1, 2009, and May 1, 2012, automatically assigned all medical audio file transcriptions to Fedtrans Transcription Services, Inc. ("Fedtrans"). Fedtrans, which is located in India, assigned respondents' files to independent typists to transcribe. 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. Following the transcription, respondents either emailed the transcript file to the customer or notified the customer to retrieve the file from respondents' computer network. Audio files and transcript files can include sensitive information from or about consumers, including children, such as: 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").

The Commission's complaint alleges that respondents misrepresented that they maintained reasonable and appropriate practices to protect consumers' personal information from unauthorized access and that respondents took reasonable steps to ensure that those engaged in transcribing medical files complied with applicable security and privacy requirements. Respondents engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. 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's network and computers used by Fedtrans's 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's security practices, such as, for example, Fedtrans's written information security program or audits or assessments Fedtrans may have had of its computer network.

The complaint further alleges that as a result of these security failures, respondents were unaware that Fedtrans used an application on its computer network that stored and transmitted medical audio and transcript 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 application and index thousands of medical transcript files that respondents had assigned to Fedtrans. The files were publicly available, and were accessed, using the search engine. The Fedtrans files, which were prepared over at least eight months, 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 highly sensitive medical information, such as information about psychiatric disorders, alcohol use, drug abuse, and pregnancy loss, and notes of examinations of children.

Information contained in the Fedtrans and other files 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. Respondents could have corrected their security failures using readily available, low-cost security measures. Consumers have no way of independently knowing about respondents' security failures and could not reasonably avoid possible harms from such failures. Accordingly, the complaint alleges that respondents failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information in audio and transcript files, which 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. The Commission alleges that this practice was, and is, an unfair act or practice.

Part I of the proposed order prohibits respondents from misrepresenting (1) the extent to which respondents use, maintain, and protect the privacy, confidentiality, security, or integrity of personal information collected from or about consumers. Part II of the proposed order requires respondents to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical,

and physical safeguards appropriate to respondents' size and complexity, nature and scope of their activities, and the sensitivity of the information collected from or about consumers. Specifically, the proposed order requires respondents to:

- designate an employee or employees to coordinate and be accountable for the information security program;

- identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks;

- design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;

- develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondents, and require service providers by contract to implement and maintain appropriate safeguards; and

- evaluate and adjust the information security program in light of the results of testing and monitoring, any material changes to operations or business arrangement, or any other circumstances that they know or have reason to know may have a material impact on its information security program.

Part III of the proposed order requires respondents to obtain within the first one hundred eighty (180) days after service of the order, and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) respondents have in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) respondents' security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of sensitive consumer, employee, and job applicant information has been protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires respondents to retain documents relating to its compliance with the order. Part V requires dissemination of the order to all current and future principals, officers, directors, managers, employees, agents, and representatives having supervisory responsibilities relating to the subject matter of the order. Parts VI and VII ensure notification to the FTC of changes in corporate status and employment status of respondents Prasad and Srivastava. Part VIII mandates that respondents submit reports to the Commission detailing its compliance with the order. Part IX provides that the order expires after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.