Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Cbr Systems, Inc., File No. 112 3120

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to Cbr Systems, Inc.

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.

Cbr collects and stores umbilical cord blood and umbilical cord tissue for potential medical use. When a pregnant woman agrees to have Cbr collect and store her umbilical cord blood or umbilical cord blood and umbilical cord tissue, Cbr collects her personal information, including, but not limited to, the following: name, address, email address, telephone number, date of birth, Social Security number, driver's license number, credit card number, debit card number, medical health history profile, blood typing results, and infectious disease marker results. During the enrollment process, Cbr also collects personal information, such as fathers' Social Security numbers, and the company collects information relating to newborn children, such as name, gender, date and time of birth, birth weight, delivery type, and adoption type (i.e., open, closed, or surrogate). Cbr may also collect limited health information for certain children and the name, address, email address, and credit card information for individuals, such as friends or family members, who contribute to the cost of collecting and storing cord blood or cord tissue. The misuse of the types of personal information Cbr collects – including Social Security numbers, dates of birth, credit card numbers, and health information – can facilitate identity theft, including existing and new account fraud, expose sensitive medical data, and lead to related consumer harms.

The Commission's complaint alleges that Cbr misrepresented that it maintained reasonable and appropriate practices to protect consumers' personal information from unauthorized access. Cbr engaged in a number of practices, however, that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. Among other things, Cbr:

(1) failed to implement reasonable policies and procedures to protect the security of consumers' personal information it collected and maintained;

(2) created unnecessary risks to personal information by (a) transporting portable media containing personal information in a manner that made the media vulnerable to theft or other misappropriation; (b) failing to adequately supervise a service provider, resulting in the retention of a legacy database that contained consumers' personal information, including consumers' names, addresses, email addresses, telephone numbers, dates of birth, Social Security numbers, drivers' license numbers, credit card numbers, and health information, in a vulnerable

format on its network; (c) failing to take reasonable steps to render backup tapes or other portable media containing personal information or information that could be used to access personal information unusable, unreadable, or indecipherable in the event of unauthorized access; (d) not adequately restricting access to or copying of personal information contained in its databases based on an employee's need for information; and (e) failing to destroy consumers' personal information for which Cbr no longer had a business need; and

(3) failed to employ sufficient measures to prevent, detect, and investigate unauthorized access to computer networks, such as by adequately monitoring web traffic, confirming distribution of anti-virus software, employing an automated intrusion detection system, retaining certain system logs, or systematically reviewing system logs for security threats.

The complaint further alleges that these failures contributed to a December 2010 incident in which hundreds of thousands of consumers' personal information was unnecessarily exposed. On December 9, 2010, a Cbr employee removed four backup tapes from Cbr's San Francisco, California facility and placed them in a backpack to transport them to Cbr's corporate headquarters in San Bruno, California, approximately thirteen miles away. The backpack contained the four Cbr backup tapes, a Cbr laptop, a Cbr external hard drive, a Cbr USB drive, and other materials. At approximately 11:35 PM on December 13, 2010, an intruder removed the backpack from the Cbr employee's personal vehicle. The Cbr backup tapes were unencrypted, and they contained consumers' personal information, including, in some cases, names, gender, Social Security numbers, dates and times of birth, drivers' license numbers, credit/debit card numbers, card expiration dates, checking account numbers, addresses, email addresses, telephone numbers, and adoption type (i.e., open, closed, or surrogate) for approximately 298,000 consumers. The Cbr laptop and Cbr external hard drive, both of which were unencrypted, contained enterprise network information, including passwords and protocols, that could have facilitated an intruder's access to Cbr's network, including additional personal information contained on the Cbr network.

The proposed order contains provisions designed to prevent Cbr from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits misrepresentations about the privacy, confidentiality, security, or integrity of personal information collected from or about consumers. Part II of the proposed order requires Cbr 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 Cbr's size and complexity, nature and scope of its activities, and the sensitivity of the information collected from or about consumers. Specifically, the proposed order requires Cbr 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 Cbr, and require service providers by contract to implement and maintain appropriate safeguards; and

- evaluate and adjust its 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 it knows or has reason to know may have a material impact on its information security program.

Part III of the proposed order requires Cbr 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) it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) its 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 Cbr to retain documents relating to its compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third-party assessments and supporting documents, Cbr must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Cbr submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed complaint or order or to modify the order's terms in any way.