[BILLING CODE: 6750-01S]

FEDERAL TRADE COMMISSION

[File No. 112 3120]

Cbr Systems, Inc.; Analysis of Proposed Consent Order to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices or unfair methods of competition. The attached Analysis to Aid Public Comment describes both the allegations in the draft complaint and the terms of the consent order -- embodied in the consent agreement -- that would settle these allegations.

DATES: Comments must be received on or before February 28, 2013.

ADDRESSES: Interested parties may file a comment at https://ftcpublic.commentworks.com/ftc/cbrsystemsconsent online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write "Cbr Systems, File No. 112 3120" on your comment and file your comment online at https://ftcpublic.commentworks.com/ftc/cbrsystemsconsent by following the instructions on the web-based form. If you prefer to file your comment on paper, mail or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Room H-113 (Annex D), 600 Pennsylvania Avenue, NW, Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Laura Roposo VanDruff (202-326-2999), Ryan M. Mehm (202-326-2918), FTC, Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement, and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Home Page (for January 28, 2013), on the World Wide Web, at http://www.ftc.gov/os/actions.shtm. A paper copy can be obtained from the FTC Public Reference Room, Room 130-H, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, either in person or by calling (202) 326-2222.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before February 28, 2013. Write "Cbr Systems, File No. 112 3120" on your comment. Your comment – including your name and your state – will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission Website, at http://www.ftc.gov/os/publiccomments.shtm. As a matter of discretion, the Commission tries to remove individuals' home contact information from comments before placing them on the Commission Website.

Because your comment will be made public, you are solely responsible for making sure that your comment does not include any sensitive personal information, like anyone's Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, like medical records or other individually identifiable health

information. In addition, do not include any "[t]rade secret or any commercial or financial information which . . . is privileged or confidential," as discussed in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2). In particular, do not include competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

If you want the Commission to give your comment confidential treatment, you must file it in paper form, with a request for confidential treatment, and you have to follow the procedure explained in FTC Rule 4.9(c), 16 CFR 4.9(c).[1] Your comment will be kept confidential only if the FTC General Counsel, in his or her sole discretion, grants your request in accordance with the law and the public interest.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it at https://ftcpublic.commentworks.com/ftc/cbrsystemsconsent by following the instructions on the web-based form. If this Notice appears at http://www.regulations.gov/#!home, you also may file a comment through that website.

If you file your comment on paper, write "Cbr Systems, File No. 112 3120" on your comment and on the envelope, and mail or deliver it to the following address: Federal Trade

[1] In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c), 16 CFR 4.9(c).

Commission, Office of the Secretary, Room H-113 (Annex D), 600 Pennsylvania Avenue, NW, Washington, DC 20580. If possible, submit your paper comment to the Commission by courier or overnight service.

Visit the Commission Website at http://www.ftc.gov to read this Notice and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before February 28, 2013. You can find more information, including routine uses permitted by the Privacy Act, in the Commission's privacy policy, at http://www.ftc.gov/ftc/privacy.htm.

Analysis of Agreement Containing Consent Order to Aid Public Comment

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 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.

By direction of the Commission.

Donald S. Clark
Secretary.

[FR Doc. 2013-02143 Filed 01/31/2013 at 8:45 am; Publication Date: 02/01/2013]