**112 3120**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

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

| | | |
|---|---|---|
| **In the Matter of** | ) | |
| | ) | **DOCKET NO. C-4400** |
| **CBR SYSTEMS, INC.** | ) | |

# COMPLAINT

The Federal Trade Commission, having reason to believe that Cbr Systems, Inc. has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Cbr Systems, Inc. ("Cbr") is a California corporation with its principal office or place of business at 1200 Bayhill Drive, Suite 301, San Bruno, California 94066.

2. The acts and practices of Cbr as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

3. At all relevant times, Cbr has been in the business of collecting and storing umbilical cord blood and tissue for potential medical use. Umbilical cord blood and tissue contain certain stem cells, the use of which researchers are investigating to treat some diseases and conditions.

4. Cbr maintains several websites through which consumers and physicians may interact with Cbr to obtain information regarding cord blood and cord tissue banking. Cbr also operates websites about pregnancy, parenting, maternity fashion, and baby names through which consumers may learn about Cbr's cord blood and cord tissue banking services. Certain Cbr websites require consumers to provide personal information to obtain a free membership.

5. When a pregnant woman agrees to have Cbr collect and store her umbilical cord blood or umbilical cord blood and cord tissue following delivery, 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 from fathers, including fathers' Social Security numbers. Cbr also collects from parents information relating to newborn children, including the following: name; gender; date and time of birth; birth weight, delivery type, and adoption type (i.e., open, closed, or surrogate). For certain children, Cbr may also collect limited health information.

6. An individual – such as a friend or family member – may contribute toward the cost of collecting and storing a pregnant woman's umbilical cord blood or umbilical cord blood and cord tissue through a service Cbr promotes as a "Gift Registry." When an individual contributes to a Gift Registry, Cbr collects personal information, including but not limited to the following: name, address, email address, and credit card information.

7. 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.

8. Between March 2006 and October 2011, Cbr disseminated or caused to be disseminated to consumers privacy policies and statements, including, but not limited, to Exhibits A through D. These materials contain the following statements:

> **Privacy Policy** (Exhibits A, B, C & D) (effective Mar. 6, 2006 through Oct. 9, 2011)
>
> Whenever CBR handles personal information, regardless of where this occurs, CBR takes steps to ensure that your information is treated securely and in accordance with the relevant Terms of Service and this Privacy Policy. . . . Once we receive your transmission, we make our best effort to ensure its security on our systems.

9. Cbr has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. Among other things, Cbr:

A. Failed to implement reasonable policies and procedures to protect the security of consumers' personal information it collected and maintained;

B. Created unnecessary risks to personal information by:

i. transporting portable media containing personal information in a manner that made the media vulnerable to theft or other misappropriation;

ii. 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;

iii. 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;

iv. not adequately restricting access to or copying of personal information contained in its databases based on an employee's need for information; and

v. failing to destroy consumers' personal information for which Cbr no longer had a business need; and

C. 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.

10. Cbr's failures to provide reasonable and appropriate security for consumers' personal information contributed to a December 2010 incident in which 298,000 consumers' personal information was unnecessarily exposed.

11. Specifically, 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.

12. 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.

## FTC ACT VIOLATIONS

13. Through the means described in Paragraph 8, Cbr represented, expressly or by implication, that it implemented reasonable and appropriate measures to protect consumers' personal information from unauthorized access.

14. In truth and in fact, as set forth in Paragraph 9, Cbr had not implemented reasonable and appropriate measures to protect consumers' personal information from unauthorized access. Therefore, the representation set forth in Paragraph 13 was, and is, false or misleading.

15. The acts and practices of Cbr as alleged in this complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

**THEREFORE**, the Federal Trade Commission, this twenty-ninth day of April, 2013, has issued this complaint against Cbr.

By the Commission.

Donald S. Clark
Secretary

SEAL