

Complaint

IN THE MATTER OF

CBR SYSTEMS, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4400; File No. 112 3120
Complaint, April 29, 2013 – Decision, April 29, 2013

The complaint alleges that Cbr Systems, Inc. (“Cbr”), a provider of umbilical cord blood and umbilical cord tissue banking services, failed to protect the security of its customers’ personal information. According to the complaint, in December 2010, a Cbr laptop, external hard drive, USB drive, and several unencrypted backup tapes were stolen from a Cbr employee’s personal vehicle, exposing the Social Security numbers and credit and debit card numbers of nearly 300,000 consumers. The complaint alleges that Cbr’s privacy policy misrepresented its efforts to protect the security of its customers’ personal information, making its privacy policy claims deceptive under the Federal Trade Commission Act. The consent order requires Cbr to establish and maintain a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information from or about consumers. The order further prohibits Cbr from engaging in future practices similar to those alleged in the complaint.

Participants

For the *Commission*: *Ryan Mehm and Laura Riposo VanDruff.*

For the *Respondent*: *Thomas F. Chaffin, Michael Sibarium, and Joseph R. Tiffany, Pillsbury Winthrop Shaw Pittman LLP.*

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.

Complaint

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.

Complaint

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,

Complaint

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

Complaint

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.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft of complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 *et seq.*;

The respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said agreement is for settlement purposes only and does not constitute an admission by respondent that the law has been violated as alleged in such complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comment filed by an interested person, now in further conformity with the procedure prescribed in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:

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

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Cbr Systems, Inc., and its successors and assigns.
2. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number or other government-issued identification number; (g) a bank account, debit card, or credit card account number; (h) a persistent identifier, such as a customer number held in a “cookie” or processor serial number; (i) clinical laboratory testing information, including test results; or (j) the fact and circumstances of a child’s adoption, such as whether the birth mother was a surrogate. For the purpose of this provision, a “consumer” shall mean any person, including, but not limited to, any user of respondent’s services, any employee of respondent, or any individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under the control of respondent.

Decision and Order

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, shall not misrepresent in any manner, expressly or by implication, the extent to which it uses, maintains, and protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this order, establish and implement, and thereafter 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 by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. This section may be satisfied through the review and maintenance of an existing program so long as that program fulfills the requirements set forth herein. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program;
- B. the identification of 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 assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk

Decision and Order

assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of the information security program in light of the results of the testing and monitoring required by subpart C, any material changes to any operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of the information security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SANS Institute; or a

Decision and Order

qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and
- D. certify that the security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been completed. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement,

Decision and Order

Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Cbr Systems, Inc.*, FTC File No.1123120. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

- A. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts II and III of this order, for the compliance period covered by such Assessment;
- B. unless covered by IV.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, a print or electronic copy of each document relating to compliance with this order, including but not limited to:
 - 1. all advertisements and promotional materials containing any representations covered by this order, with all materials used or relied upon in making or disseminating the representation; and
 - 2. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question compliance with this order.

Decision and Order

V.

IT IS FURTHER ORDERED that respondent shall deliver copies of the order as directed below:

- A. Respondent shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers, (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.
- B. Respondent shall secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by

Decision and Order

overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Cbr Systems, Inc.*, FTC File No.1123120. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports.

VIII.

This order will terminate on April 29, 2033, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as

Analysis to Aid Public Comment

though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

**ANALYSIS OF 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,

Analysis to Aid Public Comment

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'

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

**FILIQUARIAN PUBLISHING, LLC;
CHOICE LEVEL, LLC; AND JOSHUA LINSK**

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTIONS 604 AND 607 OF THE FAIR CREDIT REPORTING ACT AND
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

*Docket No. C-4401; File No. 112 3195
Complaint, April 30, 2013 – Decision, April 30, 2013*

This consent order relates to Filiquarian Publishing, LLC, Choice Level, LLC, and their owner and sole officer, Joshua Linsk (collectively “respondents”), who developed and marketed a mobile application that allowed customers to conduct an unlimited number of searches for criminal records within a particular state or county. Respondents advertised that customers could use its mobile apps to screen employees or conduct credit screenings. At the same time, however, respondents issued a disclaimer stating its mobile application was not compliant with the Federal Credit Reporting Act (FCRA) and that anyone using their mobile application for employment or credit screening purposes assumed sole responsibility for FCRA compliance. The complaint alleges that respondents failed to adhere to three key requirements of the Fair Credit Reporting Act (FCRA) (1) to maintain reasonable procedures for verifying user identity and that the information would be used for a permissible purpose; (2) to ensure that the information they provided in consumer reports was accurate; and (3) to provide adequate notice to users and to those who furnished respondents with information that was included in consumer reports. The complaint further alleges respondents’ disclaimers are insufficient to circumvent FCRA liability because the company expressly advertised that its reports could be used for employment purposes. The order requires respondents to comply with the relevant provisions of the FCRA, retain documents relating to their compliance with the order for a five year period.

Participants

For the *Commission*: *Jessica Lyon and Anthony Rodriguez.*

For the *Respondent*: *Andrea Delgadillo Ostrovsky, Calfo, Harrigan, Leyh, and Eakes.*

COMPLAINT

The Federal Trade Commission (“FTC” or “Commission”), having reason to believe that Filiquarian Publishing, LLC, Choice Level, LLC, and Joshua Linsk, individually, and as an officer of