

Complaint

**IN THE MATTER OF
CERIDIAN CORPORATION****CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT**

*Docket No. C-4325; File No. 102 3160
Filed June 8, 2011 – Decision June 8, 2011*

This consent order addresses Ceridian Corporation's ("Ceridian") web-based payroll processing service for small business customers, known as "Powerpay."

The complaint alleges that Ceridian violated Section 5 of the FTC Act by failing to provide reasonable and appropriate security for the sensitive personal information it collected and maintained. As a result of these failures, hackers executed an SQL injection attack on the Powerpay website and web application and exported the information of at least 27,673 individuals, including bank account numbers, Social Security Numbers, and dates of birth. The consent order prohibits Ceridian from misrepresenting the privacy, confidentiality, or integrity of personal information it collects from or about consumers. The consent order also requires Ceridian to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of such information about consumers, employees, and those seeking to become employees.

Participants

For the *Commission*: *Tiffany George* and *Jamie Hine*.

For the *Respondent*: *David Zetoony* and *Megan Gajewski*,
Bryan Cave LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Ceridian Corporation ("respondent") 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:

Complaint

1. Respondent Ceridian Corporation (“Ceridian”) is a Delaware corporation with its principal office or place of business at 3311 East Old Shakopee Road, Minneapolis, Minnesota 55425.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

3. Respondent is a service provider that, among other things, provides payroll processing, payroll-related tax filing, benefits administration, and other human resource services to business customers.

4. Among other things, respondent operates Powerpay, a web-based payroll processing service in the United States under the name “Powerpay.” Respondent’s small business customers enter their employees’ personal information on to the Powerpay website, which they use as a repository to collect, track, and store employee payroll data and to automate payroll processing for their employees.

5. When customers enter their employees’ personal information on to the Powerpay website, the information is sent to computers on respondent’s computer network for the purpose of computing payroll amounts and processing payroll checks and direct deposits. This personal information can consist of sensitive information about employees, including, in some instances, name, address, email address, telephone number, Social Security number, date of birth, and direct deposit account number (hereinafter “personal information”).

6. Since at least September 2008, respondent has disseminated or caused to be disseminated statements on the Ceridian website, including, but not limited to, the following statement regarding the privacy and confidentiality of the personal information they collect:

Worry-free Safety & Reliability . . . When managing employee health and payroll data, security is paramount with Ceridian. Our comprehensive

Complaint

security program is designed in accordance with ISO 27000 series standards, industry best practices and federal, state and local regulatory requirements.

7. In addition, respondent has disseminated or caused to be disseminated statements in its contracts with customers, including, but not limited to, the following statements regarding the security measures it takes to protect the personal information entrusted to its business customers:

Confidentiality and Privacy: [Ceridian] shall use the same degree of care as it uses to protect its own confidential information of like nature, but no less than a reasonable degree of care, to maintain in confidence the confidential information of the [customer].

8. Until at least December 2009, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the personal information it collected and maintained. Among other things, respondent: (1) stored personal information in clear, readable text; (2) created unnecessary risks to personal information by storing it indefinitely on its network without a business need; (3) did not adequately assess the vulnerability of its web applications and network to commonly known or reasonably foreseeable attacks, such as “Structured Query Language” (“SQL”) injection attacks; (4) did not implement readily available, free or low-cost defenses to such attacks; and (5) failed to employ reasonable measures to detect and prevent unauthorized access to personal information.

9. In December 2009, hackers exploited the failures set forth in Paragraph 8 by using a SQL injection attack on the Powerpay website and web application. Through this attack, the hackers found personal information stored in Powerpay on respondent’s network and exported the information of at least 27,673 individuals, including, in some instances, bank account numbers, Social Security Numbers, and dates of birth, over the internet to outside computers.

Complaint

10. Through the means described in Paragraphs 6 and 7, respondent represented, expressly or by implication, that it implemented reasonable and appropriate measures to protect personal information against unauthorized access.

11. In truth and in fact, respondent did not implement reasonable and appropriate measures to protect personal information against unauthorized access. Therefore, the representations set forth in Paragraphs 6 and 7 were, and are, false or misleading.

12. As set forth in Paragraph 8, respondent failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information. Respondent's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

13. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this eighth day of June, 2011, has issued this complaint against respondent.

By the Commission.

DECISION AND ORDER

The Federal Trade Commission 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 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 the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq*;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent 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 has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure described 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 Ceridian Corporation is a Delaware corporation with its principal office or place of business at 3311 East Old Shakopee Road, Minneapolis, Minnesota 55425.

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. “Personally identifiable information” or “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 or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information, including card number, expiration date, and security code; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (j) any information that is combined with any of (a) through (i) above. 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.
2. Unless otherwise specified, “respondent” shall mean

Decision and Order

Ceridian and its subsidiaries, divisions, successors and assigns, except that no provision of this Order shall apply to any foreign entity, to the extent that its conduct does not fall within the Commission's jurisdiction.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

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

II.

IT IS FURTHER ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device, 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. 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;

Decision and Order

- 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 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 failure;
- 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 respondent's information security program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's 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 its information security program.

Decision and Order

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; *provided, however*, that this Part shall not apply to Comdata Network Inc. or Ceridian Stored Value Solutions, Inc. to the extent that they do not advertise, market, promote, offer for sale, or sell any product or service relating to payroll, taxes, or human resources. *Provided further* that this Part shall not apply to payment cards provided to employers by Comdata Network Inc. that are not linked to accounts maintained by individual employees. 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 SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly 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 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

Decision and Order

meet or exceed the protections required by Part II of this order; and

- D. certify that respondent's 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 prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of 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, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Ceridian Corporation*, FTC File No.1023160. *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 print or electronic copy of:

- A. for a period of three (3) years after the date of preparation of each Assessment required under Part III of

Decision and Order

this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the 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, all other documents relating to compliance with this order, including but not limited to:
1. all advertisements and promotional materials containing any representations covered by this order, as well as 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 respondent's compliance with this order.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities.

Decision and Order

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) 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 corporation; 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 the corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation(s) about which respondent learns fewer 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 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 Ceridian Corporation*, FTC File No.1023160. *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 an additional true and accurate written report.

Decision and Order

VIII.

This order will terminate on June 8, 2031, or twenty (20) years from the most recent date that the United States or the 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 fewer 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 as to such respondent will terminate according to this Part as 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 to Aid Public Comment

**ANALYSIS OF PROPOSED CONSENT ORDER
TO AID PUBLIC COMMENT**

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to Ceridian Corporation.

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.

The Commission's complaint alleges that Ceridian is a service provider that, among other things, provides payroll processing, payroll-related tax filing, benefits administration, and other human resource services to business customers. The company operates a web-based payroll processing service for small business customers in the United States under the name "Powerpay." Ceridian's customers enter their employees' personal information on the Powerpay website, which they use to automate payroll processing for their employees.

The complaint alleges that when customers enter their employees' personal information on the Powerpay website, the information is sent to computers on Ceridian's computer network for the purpose of computing payroll amounts and processing payroll checks and direct deposits. This personal information, in some instances, consists of name, address, email address, telephone number, Social Security number, date of birth, and direct deposit account number. Such information – particularly Social Security numbers, which do not expire – can be used to facilitate identity theft, including existing and new account fraud, among other things. In addition, direct deposit account information can be used to facilitate theft.

Analysis to Aid Public Comment

The complaint alleges that Ceridian engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the personal information it collected and maintained. Among other things, Ceridian: (1) stored personal information in clear, readable text; (2) created unnecessary risks to personal information by storing it indefinitely on its network without a business need; (3) did not adequately assess the vulnerability of its web applications and network to commonly known or reasonably foreseeable attacks, such as “Structured Query Language” (“SQL”) injection attacks; (4) did not implement readily available, free or low-cost defenses to such attacks; and (5) failed to employ reasonable measures to detect and prevent unauthorized access to personal information. These practices are fundamental security failures. Each has been challenged in prior FTC data security cases, and each could have been remedied using well-known, readily available, and free or low-cost data security measures. In particular, SQL injection has been a well-known vulnerability for nearly a decade and is one of the most basic network vulnerabilities to address.

The complaint alleges that as a result of these failures, hackers executed an SQL injection attack on the Powerpay website and web application. Through this attack, the hackers found personal information stored in Powerpay on Ceridian’s network and exported the information of at least 27,673 individuals, including, in some instances, bank account numbers, Social Security Numbers, and dates of birth, over the internet to outside computers. Given the sensitive nature of the personal information exposed, the company’s failure to provide reasonable and appropriate security for this information is likely to cause consumers substantial injury as described above. That substantial injury is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. The complaint alleges that Ceridian’s failure to employ reasonable and appropriate measures to prevent unauthorized access to sensitive personal information is an unfair act or practice, and that the company misrepresented that it had implemented such measures, in violation of Section 5 of the Federal Trade Commission Act.

Analysis to Aid Public Comment

The proposed order applies to personal information that Ceridian entities within the Commission's jurisdiction collect from or about consumers and employees. It contains provisions designed to prevent Ceridian 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, or integrity of personal information collected from or about consumers. Part II of the proposed order requires Ceridian to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of such information (whether in paper or electronic format) about consumers, employees, and those seeking to become employees. The security program must contain administrative, technical, and physical safeguards appropriate to Ceridian's size and complexity, the nature and scope of its activities, and the sensitivity of the information collected from or about consumers and employees. Specifically, the proposed order requires Ceridian 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

Analysis to Aid Public Comment

information they receive from Ceridian, and require service providers by contract to implement and maintain appropriate safeguards; and

- evaluate and adjust its information security programs in light of the results of testing and monitoring, any material changes to operations or business arrangements, 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 Ceridian 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. Two Ceridian subsidiaries, Ceridian Stored Value Solutions, Inc. and Comdata Network Inc., are excluded from this requirement to the extent that they do not advertise, market, promote, offer for sale, or sell any product or service relating to payroll, taxes, or human resources. Part III does not apply to payment cards provided to employers by Comdata Network Inc. that are not linked to accounts maintained by individual employees.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires Ceridian 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, Ceridian 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 subsidiaries,

Analysis to Aid Public Comment

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 Ceridian 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 order or to modify its terms in any way.

Complaint

IN THE MATTER OF

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

*Docket No. C-4326; File No. 102 3076
Filed June 15, 2011 – Decision June 15, 2011*

This consent order addresses a security breach by Lookout Services, Inc. (“Lookout”), in which an employee gained unauthorized access to sensitive personal information, including Social Security numbers, of more than 37,000 consumers. Lookout provides a web-based computer product, known as I-9 Solution, that uses an employee’s sensitive personal information, including Social Security number, date of birth, address, and passport number, to verify that employee’s eligibility to work in the United States. The complaint alleges that Lookout misrepresented that it had implemented reasonable and appropriate security measures to protect the sensitive personal information it collected and maintained. This misrepresentation, combined with Lookout’s failure to implement such measures, constituted an unfair act or practice in violation of Section 5 of the FTC Act. The consent order prohibits Lookout from misrepresenting the privacy, confidentiality, or integrity of the personal information it collects from or about consumers. The consent order further requires Lookout to establish and maintain a comprehensive information security program. The consent order requires that Lookout retain an independent third party professional to assess this program on a biennial basis for the next 20 years.

Participants

For the *Commission*: Kristin Krause Cohen and Kandi Parsons.

For the *Respondent*: Rufus Oliver, Baker Botts L.L.P.

COMPLAINT

The Federal Trade Commission, having reason to believe that Lookout Services, Inc. (“respondent” or “Lookout”) has violated the