UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of	)	**DOCKET NO. C-**
CERIDIAN CORPORATION, a corporation.	)	

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:

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 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.

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. Respondents' 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 ___ day of ____, 2011, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary