**Analysis of Proposed Consent Order to Aid Public Comment**
***In the Matter of Ceridian Corporation, File No. 1023160***

---

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.

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.

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 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, 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.