Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of CardSystems Solutions Inc. File No. 052 3148

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from CardSystems Solutions Inc. ("CardSystems") and its successor, Solidus Networks, Inc., doing business as Pay By Touch Solutions ("Pay By Touch").

The consent agreement 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.

According to the Commission's proposed complaint, CardSystems provides merchants with products and services used in "authorization processing"-- obtaining approval for credit and debit card purchases from banks that issued the cards. Last year, it processed about 210 million card purchases, totaling more than $15 billion, for more than 119,000 small and mid-size merchants. In the course of processing these credit and debit card purchases, CardSystems collected and stored personal information about consumers, including card number and expiration date and other information, from magnetic stripes on the cards. Pay By Touch acquired CardSystems' assets on December 9, 2005, at which time CardSystems ceased doing business. Pay By Touch uses CardSystems' former employees, equipment, and technology to process transactions for the same merchants CardSystems served.

The Commission's proposed complaint alleges that CardSystems stored personal information on computers on its computer network and failed to employ reasonable and appropriate security measures to protect the information. The complaint alleges that this failure was an unfair practice because it caused or was likely to cause substantial consumer injury that was not reasonably avoidable and was not outweighed by countervailing benefits to consumers or competition. In particular, CardSystems engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information stored on its computer network. Among other things, it: (1) created unnecessary risks to the information by storing it; (2) did not adequately assess the vulnerability of its computer network to commonly known or reasonably foreseeable attacks, including but not limited to "Structured Query Language" injection attacks; (3) did not implement simple, low-cost, and readily available defenses to such attacks; (4) failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network; (5) did not use readily available security measures to limit access between computers on its network and between such computers and the Internet; and (6) failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.

The complaint further alleges that several million dollars in fraudulent purchases were made using counterfeit copies of credit and debit cards that contained the same personal information CardSystems had collected from the magnetic stripes of credit and debit cards and then stored on its computer network. After discovering the fraudulent purchases, banks cancelled and re-issued thousands of these credit and debit cards, and consumers holding these cards were unable to use them to access credit and their own bank accounts.

The proposed order applies to personal information from or about consumers that CardSystems and Pay By Touch (as CardSystems' successor) collect in connection with authorization processing. The proposed order contains provisions designed to prevent them from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires CardSystems and Pay By Touch to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information they collect from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to their size and complexity, the nature and scope of their activities, and the sensitivity of the personal information collected. Specifically, the order requires CardSystems and Pay By Touch 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 consumer information that could result in 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.

- Evaluate and adjust their information security program in light of the results of testing and monitoring, any material changes to their operations or business arrangements, or any other circumstances that they know or have to reason to know may have a material impact on the effectiveness of their information security program.

Part II of the proposed order requires that CardSystems and Pay By Touch obtain within 180 days, and on a biennial basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) they have in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order, and (2) their security program is operating with sufficient effectiveness to

provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected.

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires CardSystems and Pay By Touch to retain documents relating to their compliance with the order. Part IV requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part V requires them to notify the Commission of changes in their corporate status. Part VI mandates that CardSystems and Pay By Touch submit compliance reports to the FTC. Part VII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

This case is similar to the recent FTC cases against BJ's Wholesale Club and DSW Inc., which also involved alleged failures to secure credit and debit card information. As in those cases, CardSystems faces potential liability in the millions of dollars under bank procedures and in private litigation for losses related to the breach.

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.