052 3148

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of	)	
CARDSYSTEMS SOLUTIONS, INC., a corporation.	)	**DOCKET NO. C-4168**

COMPLAINT

The Federal Trade Commission, having reason to believe that CardSystems Solutions, Inc. ("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 CardSystems Solutions, Inc. is a Delaware corporation with its principal office or place of business at 6390 East Broadway, Tucson, Arizona 85710.

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.

VIOLATIONS OF THE FEDERAL TRADE COMMISSION ACT

3. Respondent provides merchants with products and services used to obtain authorization for credit and debit card purchases ("card purchases") from the banks that issued the cards ("issuing banks"). Last year, respondent provided authorization processing for card purchases totaling at least $15 billion for approximately 119,000 merchants. In connection with these activities, respondent uses the Internet and a web application program ("web application") to provide information to client merchants about authorizations that have been performed for them, and to provide information to prospective merchants about the services offered.

4. To obtain approval for a card purchase, merchants typically use respondent's services to: collect information from the card's magnetic stripe, including, but not limited to, customer name, card number and expiration date, a security code used to verify electronically that the card is genuine, and certain other information (collectively, "personal information"); format the information into an authorization request; and transmit the request to respondent's authorization processing computer network. From

there, respondent transmits the request to a computer network operated by or for a bank association (such as Visa or MasterCard) or another entity (such as American Express), which transmits it to the issuing bank. The issuing bank receives the request, approves or declines the purchase, and transmits its response to the merchant over the same computer networks used to process the request. The response includes the personal information that was included in the authorization request the issuing bank received.

5. Since 1998, respondent has stored authorization responses for up to thirty (30) days in one or more databases on its computer network. Each day, these databases contain as many as several million authorization responses.

6. Respondent has 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, respondent: (1) created unnecessary risks to the information by storing it in a vulnerable format for up to 30 days; (2) did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks, including but not limited to "Structured Query Language" (or "SQL") 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.

7. In September 2004, a hacker exploited the failures set forth in Paragraph 6 by using an SQL injection attack on respondent's web application and website to install common hacking programs on computers on respondent's computer network. The programs were set up to collect and transmit magnetic stripe data stored on the network to computers located outside the network every four days, beginning in November 2004. As a result, the hacker obtained unauthorized access to magnetic stripe data for tens of millions of credit and debit cards.

8. In early 2005, issuing banks began discovering several million dollars in fraudulent credit and debit card purchases that had been made with counterfeit cards. The counterfeit cards contained complete and accurate magnetic stripe data, including the security code used to verify that a card is genuine, and thus appeared genuine in the authorization process. The magnetic stripe data matched the information respondent had stored on its computer network. In response, issuing banks cancelled and re-issued thousands of credit and debit cards. Consumers holding these cards were unable to use them to access their credit and bank accounts until they received replacement cards.

9. As set forth in Paragraphs 6, 7, and 8, respondent's failure to employ reasonable and appropriate security measures to protect personal information it stored caused or is 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.

10. 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.

THEREFORE, the Federal Trade Commission this fifth day of September, 2006, has issued this complaint against respondent.

By the Commission, Commissioner Harbour recused.

Donald S. Clark
Secretary