082 3153

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)
)
DAVE & BUSTER'S, INC.,)
a corporation.) DOCKET NO. C-4291
)

COMPLAINT

The Federal Trade Commission, having reason to believe that Dave and Buster's, 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 Dave & Buster's, Inc. is a Missouri corporation with its principal office or place of business at 2481 Manana Drive, Dallas, Texas 75220.

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 owns and operates 53 restaurant/entertainment complexes in the United States under the names Dave & Buster's, Dave & Buster's Grand Sports Café, and Jillian's. Consumers pay for purchases at these stores with credit and debit cards (collectively, "payment cards"), or cash.

4. Respondent operates networks in each store ("in-store networks") as well as a corporate computer network (collectively, "networks"). These networks link corporate headquarters in the United States with each store, and, among other things, are used to process sales transactions.

5. In conducting its business, respondent routinely collects information from consumers to obtain authorization for payment card purchases. Among other things, it collects: the credit card account number, expiration date, and an electronic security code for payment card authorization (collectively, "personal information"). This information is particularly sensitive because it can be used to facilitate payment card fraud and other consumer harm.

6. To obtain payment card authorization, respondent collects personal information at its various in-store terminals, transfers the data to its in-store servers, and then transmits the data to a third-party credit card processing company.

7. In collecting and processing sensitive personal information, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks. In particular, respondent:

    (a) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by employing an intrusion detection system and monitoring system logs;

    (b) failed to adequately restrict third-party access to its networks, such as by restricting connections to specified IP addresses or granting temporary, limited access;

    (c) failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization;

    (d) failed to use readily available security measures to limit access between in-store networks, such as by employing firewalls or isolating the payment card system from the rest of the corporate network; and

    (e) failed to use readily available security measures to limit access to its computer networks through wireless access points on the networks.

8. Between April 30, 2007 and August 28, 2007 an intruder, exploiting some of the vulnerabilities set forth in Paragraph 7, connected to respondent's networks numerous times without authorization, installed unauthorized software, and intercepted personal information in transit from in-store networks to respondent's credit card processing company. After learning of the breach, respondent took steps to prevent further unauthorized access and to notify law enforcement and the credit card companies of affected consumers.

9. The breach compromised approximately 130,000 unique payment cards used by consumers in the United States. To date, issuing banks have collectively claimed several hundred thousand dollars in fraudulent charges on some of these implicated accounts.

10. As described in Paragraphs 7 through 9, respondent's failure to employ reasonable and appropriate security measures to protect personal information 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.

11. The acts and practices of respondent as alleged in this complaint constitute unfair 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 twentieth day of May, 2010, has issued this complaint against respondent.

By the Commission, Commissioner Ramirez not participating.

Donald S. Clark
Secretary