

Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Dave & Buster's, Inc., File No. 0823153

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Dave & Buster's, Inc. ("Dave & Buster's").

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.

Dave & Buster's owns and operates 53 restaurant and entertainment complexes in the United States. Consumers may pay for purchases at these locations with credit and debit cards (collectively, "payment cards") or cash. In conducting its business, Dave & Buster's routinely collects information from consumers to obtain authorization for payment card purchases, including the credit card account number, expiration date, and an electronic security code for payment authorization. This information is particularly sensitive because it can be used to facilitate payment card fraud and other consumer fraud.

The Commission's complaint alleges that since at least April 2007, Dave & Buster's engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, Dave & Buster's: (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 specific 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 using 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.

The complaint further alleges that between April 30, 2007 and August 28, 2007, an intruder, exploiting some of these vulnerabilities, connected to Dave & Buster's networks numerous times without authorization, installed unauthorized software, and intercepted personal information in transit from in-store networks to its credit card processing company. The breach compromised approximately 130,000 unique payment cards used by consumers in the United States.

The proposed order applies to personal information Dave & Buster's collects from or about consumers. It contains provisions designed to prevent Dave & Buster's from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order requires Dave & Buster's 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 collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Dave & Buster's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires Dave & Buster's 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 respondents, and require service providers by contract to implement and maintain appropriate safeguards.
- Evaluate and adjust its information security program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of its information security program.

Part II of the proposed order requires that Dave & Buster's obtain within 180 days, and on a biennial basis thereafter for ten (10) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that it has in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order; and its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected.

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires Dave & Buster's 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, Dave & Buster's must retain the documents for a period of three years after the date that each assessment is prepared. Part IV requires dissemination of the order now and in the future to principals, officers, directors, and managers

at corporate headquarters, regional offices, and at each store having responsibilities relating to the subject matter of the order. Part V ensures notification to the FTC of changes in corporate status. Part VI mandates that Dave & Buster's submit an initial compliance report to the FTC, and make available to the FTC subsequent reports. Part VII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid 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.