

Complaint

IN THE MATTER OF

DAVE & BUSTER'S, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT*Docket No. C-4291; File No. 082 3153**Filed, May 20, 2010 — Decision, May 20, 2010*

This consent order addresses Dave & Buster's, Inc.'s practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. 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. 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 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.

Participants

For the *Commission*: *Katrina Blodgett and Kate White.*

Complaint

For the *Respondents: Benita Kahn, Vorys, Sater, Seymour and Pease LLP.*

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.

Complaint

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.

Complaint

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.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

1. Respondent is a Missouri corporation with its principal office or place of business at 2481 Manana Drive, Dallas, Texas 75220.

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent and this proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this Order, the following definitions shall apply:

- A. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license number; (g) a credit card or debit card account number; (h) a persistent identifier, such as a customer number held in "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (i) any information that is combined with any of (a) through (h) above.
- B. Unless otherwise specified, "respondent" shall mean Dave & Buster's, Inc., and its subsidiaries, divisions, and affiliates owned or controlled by Dave & Buster's, Inc. and the successors and assigns of Dave & Buster's, Inc.
- C. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

Decision and Order

I.

IT IS ORDERED that respondent, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program;
- B. the identification of 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 assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

Decision and Order

- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by sub-Part C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for ten (10) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

Decision and Order

- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

Decision and Order

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying:

- A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including but not limited to documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers at corporate headquarters, regional offices, and at each store having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

Decision and Order

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however*, that with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within ninety (90) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate on May 20, 2030, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

Decision and Order

- A. any Part in this order that terminates in less than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Ramirez not participating.

**ANALYSIS OF PROPOSED CONSENT ORDER
TO AID PUBLIC COMMENT**

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

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

AGILENT TECHNOLOGIES, INC.

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT AND SEC. 7
OF THE CLAYTON ACT

Docket No. C-4292; File No. 091 0135
Filed, June 25, 2010 — Decision, June 25, 2010

This consent order addresses the \$1.5 billion acquisition by Agilent Technologies, Inc., of Varian, Inc. Agilent and Varian are the only two competitors in the market for Micro Gas Chromatography instruments. With only four suppliers, the markets for Triple Quadrupole Gas Chromatography-Mass Spectrometry and Inductively Coupled Plasma-Mass Spectrometry instruments are highly concentrated. Agilent's acquisition of Varian would leave only three suppliers, which would lessen competition in the markets for Micro GC, 3Q GC-MS and ICP-MS instruments. The order requires Agilent to: (1) divest the assets of its Micro Gas Chromatography instruments business to Inficon Group, a subsidiary of Inficon Holding AG; and (2) divest the assets of Varian's Triple Quadrupole Gas Chromatography-Mass Spectrometry and Inductively Coupled Plasma-Mass Spectrometry instruments businesses to Bruker Corp.

Participants

For the *Commission*: *Richard H. Cunningham, Lisa D. DeMarchi Sleigh, Aylin Skroejer, and James R. Weiss.*

For the *Respondents*: *Joanne C. Lewers and Robert A. Skitol, Drinker Biddle & Reath LLP.*

COMPLAINT

Pursuant to the Clayton Act and the Federal Trade Commission Act, and its authority thereunder, the Federal Trade Commission ("Commission"), having reason to believe that Respondent Agilent Technologies, Inc. ("Agilent"), a corporation subject to the jurisdiction of the Commission, has agreed to acquire Varian,