ATTORNEY GENERAL OF THE STATE OF NEW YORK
INTERNET BUREAU

IN THE MATTER OF

BARNES & NOBLE.COM, LLC

ASSURANCE OF DISCONTINUANCE

Pursuant to the provisions of Executive Law Section 63(12) and the General Business Law ("G.B.L.") Article 22-A, ELIOT SPITZER, Attorney General of the State of New York, caused an inquiry to be made into certain business practices of the Barnesandnoble.com LLC. ("BN.COM"). As a result of such inquiry, the Attorney General determines:

ATTORNEY GENERAL'S FINDINGS

1. BN.COM is a business organized under the laws of the state of Delaware in 1998, having its principal place of business located at 76 Ninth Avenue, New York, New York.

2. BN.COM is a nationally recognized internet retailer and sells books and other merchandise over the internet.

3. Since March 1997, BN.COM and its predecessors have operated a web site, located at the URL www.barnesandnoble.com (hereinafter the "BN.COM site").

4. As used in this Assurance, "personally identifiable information" or "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; (c) an e-mail address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's e-mail address; (d) a telephone number; (e) a social security number; (f) an Internet Protocol ("IP") address or host name that identifies an individual consumer; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any information, including, but not limited to client identification number or order number, that is combined with (a) through (g) above.

5. Like a number of online merchants, BN.COM, for certain periods of time has allowed BN.COM cookie-less shoppers, i.e., shoppers who have set their browsers not to accept cookies, to make purchases on the BN.COM site. BN.COM allowed "cookie-less shopping" between some time in 1998 and August 16, 2002. The method used by BN.COM to facilitate the shopping without cookies created a vulnerability to BN.COM cookie-less shoppers. The vulnerability, in certain circumstances described below, permitted unauthorized access to the BN.COM account of such BN.COM cookie-less shoppers, including access to personal information and the ability to make purchases on the BN.COM site from such accounts.

6. In instances involving an unauthorized access, the exposed personal information was the purchase history of the BN.COM cookie-less shopper, and account set-up information, including the name, billing address, and credit card information that was stored on the BN.COM site's servers for express purchases. Actual credit card numbers were not exposed.

7. The vulnerability was caused by the manner in which BN.COM allowed consumers to conduct cookie-less shopping, and usually involved the following scenario. A

BN.COM cookie-less shopper accessed the BN.COM site and proceeded to log into his account by submitting his e-mail address and password on the BN.COM site log-in page. Because such customer's browser was set not to accept cookies, BN.COM used a session identifier stored in the URL to facilitate the shopping of such customer, i.e., to allow the information stored in the URL to point to the BN.COM Cookie-less Shopper's opened BN.COM account. Prior to either logging out of his account or the expiration or automatic "timing out" of the shopper's session, the BN.COM Cookie-less Shopper copied the URL and then forwarded the URL as a link to a third party or posted the URL on a message board. If the third party recipient's or message board visitor's browser was also set not to accept cookies, and such recipient or visitor clicked on the link within the BN.COM account's session time out period, the third party or visitor would have access to the BN.COM Cookie-less Shopper's BN.COM account.

8. BN.COM attempted to mitigate the vulnerability in May 2000 when BN.COM instituted measures to shorten the "time out" period of an opened BN.COM account to 15 minutes. From some time in 1998 to March 13, 2000, the account time out period was 15 minutes; between March and May 2000, the period was extended to 2 hours. In other words, any opened BN.COM account would then close after fifteen minutes of inactivity, requiring the shopper to input his email address and password to re-open the BN.COM account. The vulnerability was later wholly eliminated, on or about August 16, 2002, when BN.COM ceased to support cookie-less shopping on the BN.COM site.

9. Consumers who visit the BN.COM site are invited to view the company's "Security Policy." At all relevant times, the Security Policy contained, among others, the following statement:

> **Password Security**
> To further secure your Personal Customer Information, we require you to create a customer password when you establish an account with us. We encourage you to use a password that is not easily guessed (i.e., don't use your name or street name). Keep your password secret; do not share it with anyone. The only way you can place an order with us online is by entering both your registered email address and password. (emphasis added)

10. Because the vulnerability provided an alternative means of access to BN.COM cookie-less shoppers' personal information on the BN.COM site, in a manner contrary to the representations and promises in the Security Policy, BN.COM violated New York G.B.L. sections 349 and 350, which prohibit deceptive business practices and false advertising. In doing so, BN.COM violated Executive Law Section 63(12), which prohibits repeated fraudulent, and/or illegal business activities.

11. **IT NOW APPEARS** that BN.COM is willing to enter into this Assurance of Discontinuance and the Attorney General is willing to accept this Assurance of Discontinuance pursuant to Executive Law Section 63(15) in lieu of commencing a statutory proceeding.

ACCORDINGLY, IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES AS FOLLOWS:

AGREEMENT

12. This Assurance of Discontinuance shall be binding on, and apply to, BN.com, its principals, officers, directors, and any individual or entity having control or oversight, now or in the future, of collection or storage of personal information either collected on or accessed through the BN.COM site, which may include BN.COM's servants, agents, employees, joint venturers, assignees, and any subsidiary, division, affiliate, or successor in interest with respect to the BN.COM site (collectively "the Company").

13. The Company shall institute supervisory procedures reasonably designed to achieve compliance with this Assurance.

14. The Company shall not, in connection with the online sale of any product or service, misrepresent in any manner, expressly or by implication, the extent to which it will maintain and protect the privacy or confidentiality of any personally identifiable information collected from consumers through the BN.COM site.

15. The Company shall within six (6) months after execution of this Assurance, 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 consumers through the BN.COM site. Such program shall contain administrative, technical, and physical safeguards appropriate to the Company's size and complexity, the nature and scope of the Company's activities, and the sensitivity of the personal information collected from 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 (whether intentional or unintentional) 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, (i) employee training and management, (ii) information systems, including network and software design, information processing, storage, transmission, and disposal, and (iii) prevention, detection, and response to attacks, intrusions, or other systems failures, (iv) as applicable, the Company' employment of third-party contractors to deliver products available to customers on the BN.COM site or provide services that affect customers' personal information;

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, and;

d. the evaluation and adjustment of the Company's information security program in light of the results of the testing and monitoring required in subparagraph c, and material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its information security program.

16. By January 31, 2005, and at least annually thereafter for a period not less than three (3) years, the Company shall conduct a written external audit review by qualified persons, which review shall monitor and document compliance with the information security program described in paragraph 15 above, evaluate the program's effectiveness and recommend changes to it, and monitor and document the conformance of the Company's practices to its representations regarding the privacy, confidentiality and security of personally identifiable information obtained from consumers through the BN.COM site. The external auditor shall be subject to the approval of the Attorney General, which approval shall not be unreasonably withheld. (In the event such approval is not provided within five (5) days of submission, the Company shall be permitted to extend the date for submission of the final audit report to the Attorney General by the number of days required for Attorney General approval.) The Company shall adjust the program and any other standards, practices or procedures in light of (i) any findings or recommendations (a) resulting from the external audit review concluding that the Company has failed to comply with paragraphs 14 or 15 above or (ii) any material changes to the Company's operations that affect the information security program. Within twenty days of receipt, the Company shall provide the Attorney General with an unaltered copy of the external auditor's report. The Company shall advise the Attorney General of any adjustments to the program or other actions taken in response to the auditor's report within thirty days of completing them.

17. The Company shall, for a period of four (4) years after the date this Assurance is executed, maintain and upon request make available to the Attorney General for

inspection and copying a print or electronic copy capable of being printed of all documents relating to compliance with this Assurance, including:

a. A sample copy of each revised version of the web page containing the Privacy Policy posted on the BN.COM site, or other document containing any representation regarding the Company's collection, use, and security of personally identifiable information from or about consumers of goods that the Company offers through the BN.COM site. Each web page copy shall be dated and contain the full URL of the web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting the information on the web. Provided, however, that after creation of any web page or screen in compliance with this Assurance, the Company shall not be required to retain a print or electronic copy of any amended web page or screen to the extent that the amendment does not affect the Company's compliance obligations under this Assurance;

b. All reports, studies, reviews, audits, audit trails, policies, training manuals, and plans, whether prepared by or on behalf of the Company, relating to the Company's compliance with the information security program required by this Assurance; and

c. Any documents, whether prepared by or on behalf of the Company, that contradict, qualify, or call into question the Company's compliance with the information security program required by this Assurance, maintained through reasonable efforts.

18. In the event the Company identifies that an event or condition materially impacting privacy, security, and integrity of consumer personal information has occurred or will occur, the Company shall take reasonable responsive actions, which may include the following:

a. Take the affected application off-line or otherwise suspend affected activity;

b. Take reasonable additional measures to secure consumer personal information from unauthorized access;

c. Investigate the causes and means of preventing the event or condition;

d. Modify the application and system to conform to industry standards and to guard against the identified risk; and

e. In circumstances where an event has occurred that results in unauthorized persons gaining access to consumers' personally identifiable information, promptly notify all consumers who are United States residents and known to have been affected.

19. The Company shall, for a period of five (5) years from the date of execution of this Assurance, deliver a copy of this Assurance to all current and future principals, officers, directors, and managers and to all current and future employees, agents, representatives, and contractors having any control or oversight of the BN.COM site, and any person receiving training pursuant to paragraph 15 of this Assurance. The Company shall deliver a copy of this Assurance to such current individuals and entities no later than thirty (30) days after the date as of which this Assurance is executed, and to such future individuals and entities no later than thirty (30) days after such individual or entity assumes such position or responsibility.

20. The Company, by certified check, shall within ten (10) days of executing this Assurance, pay the sum of Sixty Thousand Dollars ($60,000) to the New York State Department of Law as penalties and costs of investigation.

21. Within one hundred and eighty (180) days of the execution of this Assurance, the Company shall file with the Attorney General an affidavit, completed by an officer or officers of the Company knowledgeable of the Company's business practices, verifying the Company's compliance with all the terms of this Assurance, due at that time, and the Company's intention to comply with all of the terms of this Assurance not yet due at that time, along with copies of all relevant documentation.

22. Nothing in this Assurance shall be construed to deprive any consumer or other person or entity of any private right under law.

23. This Assurance shall be governed by the laws of the State of New York.

24. To the extent any cause of action arises under this Assurance, the Company irrevocably submits to the personal jurisdiction of the state or federal courts of the State of New York.

25. The Company waives all objections to the enforceability of the terms of this Assurance.

26. Should any court of competent jurisdiction decide that any term of this Assurance is invalid, void, or unenforceable, the remaining terms shall continue to be enforceable, and that court's decision shall be interpreted to preserve the enforceability of the remaining terms as much as possible.

27. The acceptance of this Assurance of Discontinuance by the Attorney General of the State of New York shall not be deemed or construed as an approval by the

Attorney General of any of the Company's activities or practices, past or present, and the Company will not make any representations to the contrary.

28. Nothing contained herein shall be construed as relieving the Company of the obligation to comply with all state and federal laws, regulations or rules, nor shall any of the provisions of this Assurance be deemed permission to engage in any act or practice prohibited by such law, regulation or rule.

29. In the event of any violation of this Assurance of Discontinuance, the Attorney General may commence an action or proceeding, under Executive Law Section 63(12), in which evidence of a violation of this Assurance of Discontinuance shall constitute prima facie evidence of a violation of the applicable law. The Company and its officers and directors expressly acknowledge that they have knowledge of the statutes referred to in this Assurance of Discontinuance and the acts or practices alleged to be in violation of those statutes.

WHEREFORE, the following signatures are affixed hereto this 28th day of April 2004.

BARNES AND NOBLE.COM, LLC.

By:

Frank Caesar
Vice President, Legal Affairs

An Officer Authorized to Sign
on Behalf of Barnes and Noble.com, LLC.

ELIOT SPITZER

Attorney General of the
State of New York
120 Broadway
New York, New York 10271-0332
(212) 416-8433

By:

Don M. Tellock
Assistant Attorney General
INTERNET BUREAU

By:

Kenneth Dreifach, April 29, 2004

Kenneth M. Dreifach
Assistant Attorney General In Charge
INTERNET BUREAU