

# State of Connecticut

GEORGE JEPSEN  
ATTORNEY GENERAL



Hartford

October 24, 2012

Gene DeFelice  
Vice President, General Counsel & Corp. Secretary  
Barnes & Noble, Inc.  
122 Fifth Avenue  
New York, NY 10011

**RE: Barnes and Noble Data Breach**

Dear Mr. DeFelice:

I write concerning a recently disclosed data breach at Barnes & Noble, Inc. ("B&N") stores that occurred sometime prior to September 14, 2012. According to published reports, tampered payment card terminals were present in some B&N stores, enabling unauthorized individuals to personal information from B&N customers. The fact that account information and PIN's were apparently obtained from a large number of B&N stores in Connecticut and other states raises serious concerns for the security of consumers' financial information.

Given the possible impact on individuals in Connecticut and elsewhere, my office is requesting detailed information on how this breach occurred, what steps have been taken to protect the affected individuals and what new procedures have been adopted to prevent future data breaches.

I request that you provide answers to the questions below. Unless otherwise noted, for the purposes of the questions below, "You" and "Your" refer to B&N. Please provide responses or documents relative to the following by November 2, 2012:

1. Please identify the total number of individuals affected by this incident. Please include a state-by-state breakdown of such total;
2. Please describe in detail the debit or payment card terminal that was reportedly tampered with or hacked into, including a description of the hardware and

software used to read, transfer and/or store payment information, and include a photograph of such terminal;

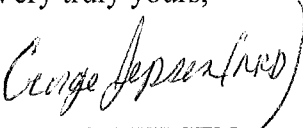
3. Please describe in detail the tampering or hacking to which this breach has been attributed, including a description of when and how You first learned of this breach;
4. Please describe the security protections, if any, employed to protect the card terminals from tampering or hacking, particularly of the sort allegedly responsible for this breach;
5. Please describe in detail all categories of personal information compromised by this breach;
6. Please identify all instances in which the personal or financial information related to or comprised in this breach of Connecticut residents was used without authorization (e.g., to make unauthorized purchases, open new accounts, etc.);
7. Please describe all steps that You have taken to ensure that all card terminals in B&N stores are secure and have not been similarly tampered with or hacked;
8. Please provide an outline of the plan You have developed to prevent the recurrence of such a breach and a timeline for implementing that plan;
9. Please provide copies of each letter sent to any financial institution, including banks, credit card companies and credit unions, notifying them of the breach;
10. Please provide the date by which You expect all notification letters to be sent to all relevant financial institutions;
11. Please provide copies of all letters or requests from law enforcement requesting or permitting You to delay the notification of this breach to affected consumers;
12. Please provide a copy of any security reports and/or forensic analyses, including any correspondence and memoranda related thereto, concerning this breach;
13. Please provide copies of Your correspondence with Visa, Inc., MasterCard Worldwide, American Express Company, and/or Discover Financial Services, concerning this breach;
14. Please provide documents regarding B&N's compliance with or failure to comply with Payment Card Industry Data Security Standard requirements;
15. Please describe all steps You have taken or will take to contact and warn consumers that their personally identifying information may have been

compromised including, but not limited to, when and how You first notified consumers of this breach, and whether You will individually notify each consumer about the breach;

16. Please describe in detail whether You have or will offer to consumers any protections from identity theft or fraud (e.g., credit monitoring, identity theft insurance, etc.);
17. Please describe Your general corporate policies regarding securing credit and debit card terminals, PIN pads, servers, and databases containing personal information, as well as Your policies regarding workforce compliance; and
18. Please identify each other instance where B&N customers' information has been subjected to unauthorized access and, for each incident, state whether any sensitive, personally identifiable information was involved.

I appreciate your cooperation in this matter and look forward to hearing from you. The information requested herein should be sent to Assistant Attorney General Matthew Fitzsimmons at 110 Sherman Street, Hartford, Connecticut 06105. Should you have any questions, you may contact AAG Fitzsimmons at 860-808-5400 or [Matthew.Fitzsimmons@ct.gov](mailto:Matthew.Fitzsimmons@ct.gov).

Very truly yours,



GEORGE JEPSEN