

---

# ARNOLD & PORTER LLP

---

Steven L. Kaplan  
Steven.Kaplan@aporter.com

+1 202.942.5998  
+1 202.942.5999 Fax

555 Twelfth Street, NW  
Washington, DC 20004-1206

October 24, 2012

**VIA FEDERAL EXPRESS**

New Hampshire Department of Justice  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

To Whom It May Concern:

On behalf of Barnes & Noble Booksellers, Inc. ("B&N"), we are providing notice in accordance with N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21 regarding a potential data breach that occurred in stores outside of New Hampshire.

B&N has detected a sophisticated criminal effort to steal credit and debit card information from its customers who swiped their cards through PIN pads when they made purchases at certain B&N retail stores. The devices used to tamper with the PIN pads may have been capable of capturing information such as name, card account number, and PIN. None of the affected PIN pads was located in a store in New Hampshire and B&N does not know of any residents of New Hampshire who have been affected.

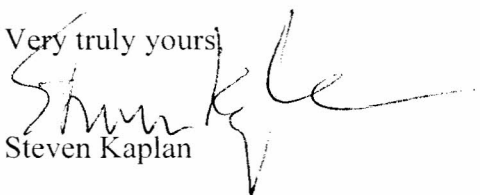
Upon discovering the breach, B&N promptly discontinued the use of all PIN pads in its nearly 700 retail stores nationwide on September 13, 2012, and began a thorough internal review involving the inspection of every PIN pad in every store. B&N has also informed federal law enforcement authorities and is cooperating with their investigation.

B&N takes its responsibility to protect its customers' privacy very seriously. B&N is implementing additional security measures designed to prevent a recurrence of the PIN pad tampering.

Out of an abundance of caution, B&N has given substitute notice through website posting and notification to major media. Attached are copies of B&N's press release and website notification.

If you have any questions or need further information, please contact me at 202-942-5998.

Very truly yours,

  
Steven Kaplan

## Important B&N Customer Notice

October 24, 2012

Dear Barnes & Noble Customers,

Barnes & Noble has just made an announcement regarding the security of personal data provided for purchases made in some of our retail stores using credit and debit card PIN pad devices. We want to make sure you are aware of the announcement, understand what happened, and know the steps that you can take if you are concerned.

We have detected a sophisticated criminal effort to steal credit and debit card information from our customers who have swiped their cards through PIN pads when they made purchases at certain retail stores. The tampered devices were capable of capturing information such as name, card account number, and PIN.

We discovered this tampering during maintenance and inspection of the devices, and we promptly discontinued the use of all PIN pads in our nearly 700 retail stores nationwide. We also informed federal law enforcement authorities, and we began a thorough internal review involving the inspection of every PIN pad in every store. Customers can make transactions securely today by asking Booksellers to swipe their cards through the card readers connected to cash registers.

We want to reassure you that this situation does not involve any purchases you may have made at Barnes & Noble.com or using your NOOK or a NOOK mobile app. The Barnes & Noble member database is secure. The tampering only affected transactions in which customers swiped their cards at one of the compromised in-store PIN pads.

If you are concerned that your card information may have been compromised, you should take the following steps:

### **Debit Card Users:**

- Change the PIN numbers on your debit cards
- Review your accounts for unauthorized transactions
- Notify your banks immediately if you discover any unauthorized purchases or withdrawals

### **Credit Card Users:**

- Review your statements for any unauthorized transactions
- Notify your card-issuing banks if you discover any unauthorized purchases or cash advances

We recommend that you remain vigilant even if you do not find any suspicious activity at this time and that you monitor your credit reports. You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. A guide with further steps you can take to protect your personal information is attached for your reference.

Barnes & Noble is cooperating with federal law enforcement in this matter. In addition, the company is working with banks, payment card brands and issuers to identify accounts that may have been compromised, so banks and issuers can employ enhanced fraud security measures on potentially impacted accounts. B&N is also implementing additional security measures designed to prevent a recurrence of such PIN pad tampering and to protect the privacy of our customers. For example, we have removed all PIN pads from our retail stores.

We value your business and B&N takes its responsibility to protect your privacy very seriously. If you have further questions about this matter, please feel free to call us at 1-888-471-7809

For your reference, the following is a copy of the press release we issued today:

#### **FOR IMMEDIATE RELEASE**

##### **CONTACTS:**

Mary Ellen Keating  
Corporate Communications  
Barnes & Noble, Inc.  
(212) 633-3323  
[mkeating@bn.com](mailto:mkeating@bn.com)

#### **BARNES & NOBLE DETECTS TAMPERING WITH PIN PAD DEVICES AT STORES**

October 24, 2012; New York – Barnes & Noble has detected tampering with PIN pad devices used in 63 of its stores. Upon detecting evidence of tampering, which was limited to one compromised PIN pad in each of the affected stores, Barnes & Noble discontinued use of all PIN pads in its nearly 700 stores nationwide. The company also notified federal law enforcement authorities, and has been supporting a federal government investigation into the matter.

Barnes & Noble has completed an internal investigation that involved the inspection and validation of every PIN pad in every store. The tampering, which affected fewer than 1% of pin pads in Barnes & Noble stores, was a sophisticated criminal effort to steal credit card information, debit card information, and debit card PIN numbers from customers who swiped their cards through PIN pads when they made purchases. This situation involved only purchases in which a customer swiped a credit or debit card in a store using one of the compromised PIN pads.

The company emphasized that its customer database is secure. Purchases on Barnes & Noble.com, NOOK and NOOK mobile apps were not affected. The member database was also not affected. None of the affected PIN pads was discovered at Barnes & Noble College Bookstores.

Barnes & Noble is continuing to assist federal law enforcement authorities in this matter. In addition, the company is working with banks, payment card brands and issuers to identify accounts that may have been compromised, so banks and issuers can employ enhanced fraud security measures on potentially impacted accounts.

The criminals planted bugs in the tampered pin pad devices, allowing for the capture of credit card and pin numbers. Barnes & Noble disconnected all pin pads from its stores nationwide by close of business September 14, and customers can securely shop with credit cards through the company's cash registers. Barnes & Noble said it is committed to providing customers with a safe shopping environment.

Tampered pin pads were discovered from stores in the following states: CA, CT, FL, NJ, NY, IL, MA, PA, RI. A complete list of specific stores follows.

Store Address	City	State	Zip
4735 Commons Way	Calabasas	CA	91302
2470 Tuscany Street Suite 101	Corona	CA	92881
2015 Birch Road Suite 700	Chula Vista	CA	91915
313 Corte Madera Town Center	Corte Madera	CA	94925
5604 Bay Street	Emeryville	CA	94608
810 West Valley Parkway	Escondido	CA	92025
1315 E. Gladstone Street	Glendora	CA	91740
5183 Montclair Plaza Lane	Montclair	CA	91763
894 Marsh St Bldg G	San Luis Obispo	CA	93401
2615 Vista Way	Oceanside	CA	92054
72-840 Highway 111 Suite 425	Palm Desert	CA	92260
27460 Lugonia Ave	Redlands	CA	92374
1150 El Camino Real Space 277	San Bruno	CA	94066
10775 Westview Parkway	San Diego	CA	92126
3600 Stevens Creek Blvd	San Jose	CA	95117
11 West Hillsdale Blvd.	San Mateo	CA	94403
9938 Mission Gorge Road	Santee	CA	92071
40570 Winchester Rd	Temecula	CA	92591
4820 Telephone Road	Ventura	CA	93003
1149 S. Main St.	Walnut Creek	CA	94596
470 Universal Drive North	North Haven	CT	06473
100 Greyrock Place Suite H009	Stamford	CT	06901
60 Isham Road	W. Hartford	CT	06107

18711 NE Biscayne Blvd	Aventura	FL	33180
333 N. Congress Avenue	Boynton Beach	FL	33436
152 Miracle Mile	Coral Gables	FL	33134
1900 W International Spdway	Daytona Beach	FL	32114
2051 N. Federal Highway	Fort Lauderdale	FL	33305
12405 N Kendall Drive	Miami	FL	33186
11380 Legacy Ave	Palm Beach Gardens	FL	33410
14572 SW 5th St Suite 10140	Pembroke Pines	FL	33027
11820 Pines Blvd	Pembroke Pines	FL	33026
5701 Sunset Drive Suite 196	S. Miami	FL	33143
700 Rosemary Ave Unit #104	West Palm Beach	FL	33401
1441 West Webster Avenue	Chicago	IL	60614
1130 North State Street	Chicago	IL	60610
5380 Route 14	Crystal Lake	IL	60014
20600 North Rand Road	Deer Park	IL	60010
728 North Waukegan Road	Deerfield	IL	60015
1630 Sherman Avenue	Evanston	IL	60201
1468 Springhill Mall Blvd	W. Dundee	IL	60118
170 Boylston Street	Chestnut Hill	MA	02467
96 Derby Street Suite 300	Hingham	MA	02043
82 Providence Highway	East Walpole	MA	2032
395 Route 3 East	Clifton	NJ	07014
55 Parsonage Road	Edison	NJ	08837
2134 State Highway 35	Holmdel	NJ	07733
4831 US Hwy 9	Howell	NJ	07731
23-80 Bell Blvd.	Bayside	NY	11360
176-60 Union Turnpike	Fresh Meadows	NY	11366
1542 Northern Blvd	Manhasset	NY	11030
160 E 54th Street (Citicorp)	New York	NY	10022
2289 Broadway	New York	NY	10024
33 East 17th Street (Union Square)	New York	NY	10003
555 Fifth Ave	New York	NY	10017
2245 Richmond Avenue	Staten Island	NY	10314
230 Main St	White Plains	NY	10601
97 Warren Street	New York	NY	10007
100 West Bridge Street	Homestead	PA	15120
800 Settlers Ridge Center Drive	Pittsburgh	PA	15205
1311 West Main Road	Middleton	RI	02842
371 Putnam Pike Suite 330	Smithfield	RI	02917
1350-B Bald Hill Rd	Warwick	RI	02886

As a precaution, customers and employees who have swiped their cards at any of the Barnes & Noble stores with affected PIN pads should take the following steps:

**Debit Card Users:**

- Change the PIN numbers on their debit cards
- Review their accounts for unauthorized transactions
- Notify their banks immediately if they discover any unauthorized purchases or withdrawals

**Credit Card Users:**

- Review their statements for any unauthorized transactions
- Notify their card-issuing banks if they discover any unauthorized purchases or cash advances

For additional information and updates, visit the Barnes & Noble website at [www.barnesandnobleinc.com](http://www.barnesandnobleinc.com). Customers may also call 1-888-471-7809, between the hours 8:00 AM and 8:00 PM Eastern Standard Time, with questions.

# # #

## **Steps You Can Take to Further Protect Your Information**

B&N is providing this reference guide to assist our customers who believe their account information may have been compromised. We encourage customers to remain vigilant, review payment card account statements, monitor credit reports, and consider these additional steps.

### Review Your Account Statements

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission ("FTC").

To file a complaint with the FTC, go to [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

### Credit Reports

To order a free copy of your credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the FTC website at <http://www.ftc.gov/bcp/edu/resources/forms/requestformfinal.pdf> and mail it to

Annual Credit Report Request Service,  
P.O. Box 105281,  
Atlanta, GA 30348-5281

The three national credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be internal review and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

### Consulting the FTC

If you detect any incident of fraud, promptly report the incident to your local law enforcement authority, your state Attorney General and the FTC. If you believe your account has been compromised, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. When you dispute new unauthorized accounts, use the FTC's ID Theft Affidavit, which is available at <http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the crime.

You can contact the FTC to learn more about how to protect yourself:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/)

### Police Report

If you find suspicious activity on your credit reports or account statements, or have reason to believe that your personal information is being misused, contact your local law enforcement authorities immediately and file a police report. You have the right to request a copy of the police report and should retain it for further use, as creditors may request such documentation to waive your potential liabilities in connection with fraudulent activity.

### Fraud Alerts

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert notifies you of an attempt by an unauthorized person to open a new credit account in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a free fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. You can also place a fraud alert on your credit report online at the websites listed below.

Equifax	Experian	TransUnion
Phone: 800-525-6285	Phone: 888-397-3742	Phone: 800-680-7289
P.O. Box 105069	P.O. Box 9532	P.O. Box 6790 Fullerton, CA 92634-6790



Atlanta, GA 30348-5069  <a href="http://www.equifax.com/answers/set-fraud-alerts/en_cp">http://www.equifax.com/answers/set-fraud-alerts/en_cp</a>	Allen, TX 75013  <a href="https://www.experian.com/fraud/center_rd.html">https://www.experian.com/fraud/center_rd.html</a>	<a href="https://fraud.transunion.com">https://fraud.transunion.com</a>
---	--	---

### Security Freeze

Some state laws allow you to place a security freeze on your credit reports. A security freeze would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should be aware, however, that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. The specific costs and procedures for placing a security freeze vary by state, but this Reference Guide provides general information. You can find additional information at the websites of any of the three credit reporting agencies listed below.

If you believe that you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, the agency will not charge you to place, lift or remove a security freeze on your credit reports. In all other cases, a credit reporting agency may charge you a fee, which generally ranges from \$5.00 to \$20.00 per action.

Requirements vary by state, but generally you may place a security freeze on your credit report by sending a written request to each of the three credit reporting agencies noted below, which may require the following information to verify your identity:

- (1) full name (including middle initial as well as Jr., Sr., II, III, etc.);
- (2) social Security number;
- (3) date of birth;
- (4) addresses for the prior five years;
- (5) proof of current address; and
- (6) a legible copy of a government issued identification card.

You also may provide a copy of any relevant police report, investigative report, or complaint to a law enforcement agency concerning the incident.

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
Phone: 800-525-6285  P.O. Box 105788 Atlanta, Georgia 30348  <a href="http://www.equifax.com/answers/help/security-freeze/en_cp">http://www.equifax.com/answers/help/security-freeze/en_cp</a>	Phone: 888-397-3742  Experian Security Freeze P.O. Box 9554 Allen, TX 75013  <a href="http://www.experian.com/freeze">www.experian.com/freeze</a>	Phone: 888-909-8872  P.O. Box 6790 Fullerton, CA 92634-6790  <a href="https://freeze.transunion.com">https://freeze.transunion.com</a>

### Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (877-438-4338).

A copy of Take Charge: Fighting Back Against Identity Theft, a comprehensive guide from the FTC to help you guard against and deal with identity theft, is available at [www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.shtm](http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.shtm).

### For North Carolina Residents

You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
877-566-7226 (toll-free in North Carolina)  
919-716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)

### For Maryland Residents.

You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
888-743-0023 (toll-free in Maryland)  
410-576-6300  
<http://www.oag.state.md.us>

### For Massachusetts Residents.

The credit bureaus may charge you a fee of up to \$5.00 to place a security freeze on your account, and may require that you provide proper identification prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit bureaus with a valid police report.

You have the right to obtain a police report regarding the breach.