IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ELIZABETH NOWAK, on behalf of herself and all others similarly situated,	)	
	)	Case No.
Plaintiff,	)	
v.	)	
BARNES & NOBLE, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Elizabeth Nowak ("Nowak" or "Plaintiff"), individually and on behalf of all others similarly situated, by and through her counsel, brings this Class Action Complaint against Defendant Barnes & Noble, Inc. ("Defendant" or "Barnes & Noble"). Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, alleges as follows upon personal knowledge as to herself and her own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Barnes & Noble for its failure to secure and safeguard its customers' personal financial data – including but not limited to credit and debit card information and personal identification numbers ("PIN") – and for failing to provide clear, conspicuous, and timely notice to Plaintiff and the other members of the Class that their information had been stolen.

2. On October 23, 2012, nearly six weeks after Barnes & Noble allegedly discovered what it has described as 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," Barnes & Noble began disclosing to the public that these

alleged criminals (referred to herein as "skimmers") infiltrated Barnes & Noble's flawed payment security system by tampering with PIN Pad devices at 63 separate Barnes & Noble stores, enabling them to steal Barnes & Noble's customers' personal financial data (the "Security Breach").

3. Barnes & Noble's security failures enabled the skimmers to steal financial data from within Barnes & Noble's stores and subsequently make unauthorized purchases on customers' credit cards and otherwise put Class members' financial information at serious and ongoing risk. The skimmers continue to use the information they obtained as a result of Barnes & Noble's inadequate security to exploit and injure Class members across the United States.

4. The Security Breach was caused and enabled by Barnes & Noble's knowing violation of its contractual obligations to abide by best practices and industry standards concerning the security of PIN pad terminals. Barnes & Noble grossly failed to comply with security standards and allowed their customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

5. Barnes & Noble failed to disclose the extent of the Security Breach and failed to individually notify each of its affected customers of the Security Breach in a timely manner, and failed to take other reasonable steps to clearly and conspicuously inform its customers of the nature and extent of the Security Breach. By failing to provide adequate notice, Barnes & Noble prevented (and continues to prevent) Class members from protecting themselves from the Security Breach.

6. Accordingly, Plaintiff, on behalf of herself and other members of the Class, asserts claims for breach of implied contract and violation of the Illinois Consumer Fraud and

Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*., and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

7. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of States other than Barnes & Noble's State of citizenship.

8. This Court has personal jurisdiction over Barnes & Noble because Barnes & Noble is registered with the Illinois Secretary of State to conduct business in the State of Illinois, and does conducts substantial business in the State of Illinois, such that Barnes & Noble has significant continuous and pervasive contacts with the State of Illinois. Barnes & Noble also maintains numerous stores and employees in the State of Illinois, including multiple stores compromised in the Security Breach.

9. Venue is proper in this District pursuant to 28 U.S.C. §§ 1301(a)(2), 1391(b)(2), and 1391(c)(2) as: a substantial part of the events and/or omissions giving rise to the claims emanated from activities within this District, and Barnes & Noble conducts substantial business in this District.

III. PARTIES

Plaintiff

10. Elizabeth Nowak is a citizen of Illinois and resides in Cook County, Illinois. Nowak shopped at a Barnes & Noble retail location in Illinois prior to September 14, 2012. On at least one of those occasions, Nowak swiped her debit card through one of the store's PIN pad

terminals and, as a result, entered into an implied contract with Barnes & Noble for the adequate protection of her debit card information, and had her sensitive financial information exposed as a result of Barnes & Noble's inadequate security. Barnes & Noble did not provide Nowak with timely or effective notification about the Security Breach.

Defendant

11. Barnes & Noble, Inc. is a Delaware corporation with its principal place of business in New York, New York. Barnes & Noble is America's largest book retailer, operating nearly 700 retail stores across the country.

IV. FACTUAL BACKGROUND

PIN Pad "Skimming"

12. Like many other retailers, Barnes & Noble uses PIN pad terminals to process its customers' in-store debit and credit card payments.

13. A PIN pad is an electronic device used in a debit or credit card-based transaction. To make a debit or credit card purchase through a PIN pad, a cardholder swipes their credit or debit card through the PIN pad and then inputs their PIN. A properly operating PIN pad will then encrypt the cardholder's PIN, temporarily store the encrypted PIN – along with other card and transaction information – and then transmit that information to a transaction manager or bank for verification to complete the transaction.

14. "Skimming" is a form of electronic system hacking that enables the unauthorized capture of debit and/or credit card magnetic strip data by unauthorized persons. These unauthorized persons are often referred to as "skimmers." In order to make use of the magnetic strip data on a debit card, skimmers generally require knowledge of the cardholders' PIN number.

15. Once skimmers acquire a cardholder's magnetic strip information and PIN number, they may then use that information to commit identity theft and other fraudulent scams, including but not limited to selling that information online or using it to create a fraudulent duplicate card. Skimmers can create duplicate cards in seconds, using card cloning hardware that can be purchased online. With the duplicate in hand, skimmers or their confederates use the fraudulent duplicate card together with the stolen PIN to make unauthorized purchases or withdraw cash directly from the victim's bank accounts via an ATM.

16. One method that skimmers use to obtain their victims' credit and debit card information and PIN numbers involves implanting small electronic detection devices, or "bugs," within the physical PIN pads themselves. Using this method, the skimmers are able to extract the customer's payment card information and PIN numbers when the customer swipes his or her card through the PIN pad terminal. Because the exterior of an inadequately secured PIN pad typically shows no evidence of the modification – which is entirely inside the machine – this form of tampering can be particularly hard to detect and often go unnoticed for an extended period of time.

17. The payment card industry, the PIN Pad industry, and merchants have been aware of this method for some time, however, and have developed industry best practices and contractual standards that provide greater PIN pad security (including, but not limited to tamper proof seals on PIN Pad devices, proper employee supervision of PIN Pad devices, and regular PIN Pad inspections) that help protect against this type of unauthorized PIN Pad tampering method.

Barnes & Noble's Contractual Obligation to Protect Customer Information

18. Barnes & Noble accepts customer payments for purchases through credit and debit cards issued by members of the payment card industry ("PCI") such as Visa USA ("Visa"), MasterCard, Discover, and American Express. Some card issuers, like Visa, contractually obligate merchants, like Barnes & Noble, to comply with various PIN pad security standards that protect customer financial information as a condition of being permitted to process transactions through the card issuer.

19. At all times relevant to this action, Barnes & Noble was authorized by Visa to accept Visa credit and debit cards for the payment of personal goods.

20. Visa is a privately-held for profit association that supplies and supports Visa credit and debit cards issued by financial institutions to their customers by providing an authorization service for Visa card transactions and a clearing and settlement service to transfer payment information between parties involved in credit and debit card transactions. Visa is a member of the PCI.

21. In 2005, Visa issued a global mandate ("Visa's Global Mandate"), requiring that by July 1, 2010, each of its merchants authorized to accept payment through Visa debit and credit cards discontinue the use of PIN pad terminals that do not meet the Triple Data Encryption Standard ("TDES"). TDES compliant devices provide greater security than earlier generation devices. With respect to the enhanced security protections of Visa's Global Mandate, David Ottenheimer, a payments security expert who works with the technology consultancy K3DES LLC recently noted the importance of upgrading to tamper resistant equipment, stating: "If you have a device that's five years old, it probably doesn't have the protections that it would need" to ward off fraud.

22. Barnes & Noble is contractually obligated to fully comply with Visa's Global Mandate as a condition of being permitted to process transactions through the Visa network.

23. Visa also created operating regulations for merchants who elect to accept its cards, which include a list of thirty-two requirements that those merchants must implement to protect the security of cardholder information (the "PCI PIN Security Requirements").[1]

24. The PCI PIN Security Requirements, include the following:

- Requirement 1. "All cardholder-entered PINs are processed in equipment that conforms to the requirements for tamper-resistant security modules."

- Requirement 29. "PIN-processing equipment is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys." Visa further notes that, in compliance with international and industry standards, merchants must implement procedures that "***include ensuring that a counterfeit device possessing all the correct operational characteristics plus fraudulent capabilities has not been substituted for a legitimate device***."

- Requirement 32. "Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN-processing equipment placed into service, initialized, deployed, used, and decommissioned."

25. Barnes & Noble is contractually obligated to fully comply with the PCI PIN Security Requirements as a condition of being permitted to process transactions through the Visa network.

26. Visa warns that "merchant non-compliance (with the PCI PIN Security Requirements) could potentially subject the Visa payment system to an extremely high level of risk."[2] Similarly, a merchant's non-compliance with the PCI PIN Security Requirements subjects its customers to an extremely high level of risk.

[1] *See* Payment Card Industry PIN Security Requirements, version 2.0 January 2008, located at https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=322 (last visited October 26, 2012).

[2] *See* PIN Security, Tools and Best Practices for Merchants, at 3, located at http://usa.visa.com/download/merchants/pin-security-080507-final.pdf (last visited October 26, 2012).

27. In 2006, Visa, MasterCard, and other PCI members established the Security Standards Council ("PCI SSC"). PCI SSC is an open global forum responsible for the development, management, education, and awareness of PCI Data Security Standard and related standards for increased security of PIN pad terminals.

28. In addition to developing security standards applicable to payment card processing generally, PCI SSC developed even more stringent standards for PIN pad terminals (referred to by the PCI SSC as "PCI PIN Entry Devices" or "PCI PEDs") in order, among other things, to make PIN pad terminals more tamper-resistant.[3]

29. Since December 31, 2007, PCI members require that merchants who accept their credit or debit cards do not put into service PIN pad terminals that fail to meet the PCI PED standard.[4]

30. Barnes & Noble is contractually obligated – as a condition of being permitted to process transactions through PCI companies – to fully comply with the PCI PED requirements and other requirements concerning the security of customer financial information.

Industry Standard Practices

31. PCI SCC, PIN pad manufacturers, and credit card processors have developed and implemented a series of "best practices" for merchants to prevent or identify instances of PIN pad tampering.

32. PCI SCC practices for preventing PIN pad terminal tampering include but are not limited to logging the serial numbers of the PIN pad terminals in the store and periodically inspecting those devices to ensure that they have not been substituted with tampered terminals.[5]

[3] *See* Payment Card Industry PIN Security Requirements, version 2.0, January 2008 at 77.
[4] *Id.*

33. Similarly, VeriFone, a leading manufacturer of PIN pad terminals warned merchants including Barnes & Noble that older PIN pads can be tampered or "bugged" by skimmers and issued a series of best practices to increase security of PIN pad terminals.[6] The document notes:

> We are seeing an increase in criminal organizations targeting the less secure pre PED terminals by installing bugs to collect private credit card and debit information. In these cases, the criminal organizations are inserting a bug into an in-place device or obtaining the same terminal model that a retailer uses, installing a bug, and then substituting the tampered device for the retailer's terminals. They then either come back to retrieve these terminals to obtain the stolen information, or in some cases, the tampered terminals send the information to another computer via wireless communications.
>
> Due to repeated targeting of pre PED PIN pads and payment terminals, VeriFone has developed the following PIN Pad Security Best Practices. These best practices first enable a retailer to determine if any existing terminals have been tampered with, and second make tampering much more difficult by implementing a comprehensive set of security controls to prevent tampering and more quickly become aware if tampering has occurred.[7]

34. VeriFone's best practices include educating employees about skimming practices, preventing the unauthorized tampering or bugging of PIN pad terminals, and visually inspecting the terminals for signs of tampering.[8]

35. Steve Elefant, Chief Information Officer of credit card processor Heartland Payment Systems, noted that "[o]ne of the best practices stores need to think about is keeping track of the devices they have through video and individual employees, and verifying that people

---

[5] *See* PCI Security Standards Council: Security Program Requirements and PCI Data Security Standard, located at https://www.pcisecuritystandards.org/documents/skimming_prevention_IS.pdf (last visited October 26, 2012).

[6] *See* VeriFone PIN Pad Security Best Practices v2, at 2, located at http://www.posdata.com/documents/PIN_Pad_Security_Best_Practices_V2.pdf (last visited October 26, 2012).

[7] *Id.* at 2.

[8] *Id.* at 3.

aren't . . . putting a skimmer in." Heartland Payment Systems offers PIN pad terminals to merchants that immediately discontinue service "the second they're modified." The company also monitors back-end traffic emanating from its PIN pads for unusual activity, such as unencrypted transactions.

36. Merchants that use modern PIN pad terminals and follow the requirements, standards, and best practices outlined above can protect their customers from security breaches like the one at issue here.

Security Breaches Lead to Identity Theft

37. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[9] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records...[and their] good name."

38. According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[10] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[11]

[9] *See* http:///www.gao.gov/new.items/d07737.pdf.

[10] *See* FTC Identity Theft Website: www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[11] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security

39. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

40. Personal identifying information ("PII") – like the Barnes & Noble's customer names combined with their credit or debit card information that were stolen in the Security Breach at issue in this action– is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[12] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, and other PII directly on various Internet websites making the information publicly available.

The Barnes & Noble Skimming Scam

41. On October 23, 2012 – almost six weeks after Barnes & Noble allegedly discovered the wrongful conduct at issue in this litigation– Barnes & Noble reported that PIN pad tampering occurred in 63 of its stores, including seven of its Chicago-area stores. Barnes & Noble also revealed that prior to September 14, 2012, skimmers tampered with one device in each of those 63 stores, which are located in nine states. According to Barnes & Noble, the

---

number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[12] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009).

security breach affected PIN pad terminals at stores in California, Connecticut, Florida, Illinois, Massachusetts, New Jersey, New York, Pennsylvania, and Rhode Island.

42. Barnes & Noble has reported that it does not know how many customers were affected by the Security Breach, and insists that its customer database has been secured. Yet Barnes & Noble acknowledges that the skimmers have, ***in fact***, made numerous unauthorized purchases on Class Members' credit cards.[13]

43. Upon information and belief, at the time of the Security Breache, Barnes & Noble was not in compliance with Visa's Global Mandate that requires the use of tamper-resistant PIN pads in all of its stores. Barnes & Noble also failed to comply with the PCI PIN Security Requirements.

44. Barnes & Noble's failure to comply with Visa's Global Mandate and the PCI PIN Security Requirements provided Barnes & Noble with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of Barnes & Noble's own customers – including Class members here – who have been subject to the Security Breach or otherwise have had their financial information placed at serious and ongoing risk.

45. Barnes & Noble allowed widespread and systematic theft of its customers' financial information. Barnes & Noble's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information. Despite being contractually obligated to do so, Barnes & Noble failed to employ appropriate technical, administrative, or physical procedures to protect its customers' financial information from unauthorized capture, dissemination, or misuse, thereby making its customers easy targets

[13] http://www.nytimes.com/2012/10/24/business/hackers-get-credit-data-at-barnes-noble.html?_r=0 (last visited October 26, 2012).

for theft and misuse of their financial information, including in the manner undertaken by the skimmers here.

Barnes & Noble Fails To Provide Sufficient Notice of The Data Breach To Class Members

46. Barnes & Noble's customers are subject to continuing damage from having their personal information compromised due to Barnes & Noble's inadequate security. Barnes & Noble's customers were and are entitled to clear, conspicuous, and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud as alleged herein. Barnes & Noble, however, has failed to take reasonable steps to notify its customers that their information has been compromised.

47. Barnes & Noble has failed to directly notify individual Class members about the data breach, and has also failed to post signs in each of its affected stores to notify its returning customers that their financial information may have been compromised, that the skimmers may have stolen their debit and/or credit card information, and that, as a result of this data theft, customers may be at risk of unauthorized credit and/or debit card charges and other fraudulent activity in the future.

48. On October 23, 2012 – almost six weeks after Barnes & Noble allegedly first learned of the PIN pad terminal tampering – Barnes & Noble finally notified the press that a data breach occurred in its Chicago-area stores and more than 50 others.

49. The following day, Barnes & Noble posted a notice on its website stating that it had "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."[14] The notice further states that Barnes & Noble "discovered this tampering during maintenance and inspection of the devices," and then worked with law enforcement to investigate the breach and conduct a "thorough internal review" of the PIN pads.[15]

50. Although the notice contains language designed to reassure the reader that "[c]ustomers can make transactions securely today by asking booksellers to swipe their cards,"[16] Barnes & Noble fails to acknowledge their failure to implement proper security measures *prior* to the breach – when it actually matters.

51. Rather than take responsibility for its security failures that resulted in the Security Breach, Barnes & Noble has placed the burden on aggrieved customers like Plaintiff and the other members of the Class, either to self-monitor their accounts and credit reports for years to come, or to spend time and money on fraud alerts or credit-report security freezes.

52. ***At no time*** has Barnes & Noble offered credit monitoring or identity theft protection assistance to Plaintiff or the other members of the Class, nor has Barnes & Noble taken any affirmative steps to make Class members whole for the damages arising out of Barnes & Noble's conduct.

V. CLASS ACTION ALLEGATIONS

53. Plaintiff brings Count I, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in the United States who made an in-store purchase at a Barnes & Noble store using a debit or credit card that was swiped through a PIN pad at any time from November 1, 2010 through the present (the "National Class").

[14] *See Important Customer Notice*, http://www.barnesandnobleinc.com/newsroom/customer_notice.html (last visited Oct. 25, 2012).
[15] *Id.*
[16] *Id.*

Excluded from the National Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

54. Plaintiff brings Count II, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All persons residing in one of the Consumer Fraud States[17] who made an in-store purchase at a Barnes & Noble store using a debit or credit card that was swiped through a PIN pad at any time from November 1, 2010 through the present (the "Consumer Fraud Multistate Class").

Excluded from the Consumer Fraud Multistate Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

55. In the alternative, Plaintiff brings Count II, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

[17] The States with similar consumer fraud laws under the facts of this case are: Arkansas (Ark. Code § 4-88-101, et seq.); Colorado (Colo. Rev. Stat. § 6-1-101, et seq.); Connecticut (Conn. Gen. Stat. § 42-110, et seq.); Delaware (Del. Code tit. 6, § 2511, et seq.); District of Columbia (D.C. Code § 28-3901, et seq.); Florida (Fla. Stat. § 501.201, et seq.); Georgia (GA Code § 10-1-390 et seq.); Hawaii (Haw. Rev. Stat. § 480-1, et seq.); Idaho (Idaho Code § 48-601, et seq.); Illinois (815 Ill. Comp. Stat. 502/1, et seq.); Maine (Me. Rev. Stat. tit. 5 § 205-A, et seq.); Massachusetts (Mass. Gen. Laws Ch. 93A, et seq.); Michigan (Mich. Comp. Laws § 445.901, et seq.); Minnesota (Minn. Stat. § 325F.67, et seq.); Missouri (Mo. Rev. Stat. § 407.010, et seq.); Montana (Mo. Code. § 30-14-101, et seq.); Nebraska (Neb. Rev. Stat. § 59-1601, et seq.); Nevada (Nev. Rev. Stat. § 598.0915, et seq.,); New Hampshire (N.H. Rev. Stat. § 358-A:1, et seq.); New Jersey (N.J. Stat. § 56:8-1, et seq.); New Mexico (N.M. Stat. § 57-12-1, et seq.); New York (N.Y. Gen. Bus. Law § 349, et seq.); North Dakota (N.D. Cent. Code § 51-15-01, et seq.); Oklahoma (Okla. Stat. tit. 15, § 751, et seq.); Oregon (Or. Rev. Stat. § 646.605, et seq.); Rhode Island (R.I. Gen. Laws § 6-13.1-1, et seq.); South Dakota (S.D. Code Laws § 37-24-1, et seq.); Virginia (VA Code § 59.1-196, et seq.); Vermont (Vt. Stat. tit. 9, § 2451, et seq.); Washington (Wash. Rev. Code § 19.86.010, et seq.); West Virginia (W. Va. Code § 46A-6-101, et seq.); and Wisconsin (Wis. Stat. § 100.18, et seq.) (collectively, the "Consumer Fraud States").

> All persons residing in the State of Illinois who made an in-store purchase at a Barnes & Noble store using a debit or credit card that was swiped through a PIN pad at any time from November 1, 2010 through the present (the "Illinois State Class")

Excluded from the Illinois State Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

56. The National Class, Consumer Fraud Multistate Class, and Illinois State Class are collectively referred to as the "Class," unless specifically indicated otherwise.

57. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

58. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the thousands. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from Barnes & Noble's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

59. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether Barnes & Noble failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive financial information;

b. Whether Barnes & Noble properly implemented its purported security measures to protect customer financial information from unauthorized capture, dissemination, and misuse;

c. Whether Barnes & Noble took reasonable measures to determine the extent of the Security Breach after it first learned of same;

d. Whether Barnes & Noble's delay in informing consumers of the Security Breach was unreasonable;

e. Whether Barnes & Noble's method of informing consumers of the security breach and its description of the breach and potential exposure to damages as a result of same was unreasonable;

f. Whether Barnes & Noble's conduct violates the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*;

g. Whether Barnes & Noble's conduct constitutes breach of an implied contract;

h. Whether Barnes & Noble's conduct constitutes unjust enrichment; and

i. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

60. Barnes & Noble engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

61. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members

were comparably injured through Barnes & Noble's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Barnes & Noble that are unique to Plaintiff.

62. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation; and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and her counsel.

63. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Barnes & Noble. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

64. **Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Barnes & Noble has acted or refused to act on grounds generally applicable to Plaintiff and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

65. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Barnes & Noble, so it would be impracticable for Class members to individually seek redress for Barnes & Noble's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED

COUNT I
Breach of Implied Contract
(On Behalf of the National Class)

66. Plaintiff incorporates paragraphs 1-65 as if fully set forth herein.

67. Barnes & Noble's customers who intended to make in-store purchases with debit or credit cards were required to provide their card's magnetic strip data and PINs (for debit cards) for payment verification.

68. In providing such financial data, Plaintiff and the other members of the Class entered into an implied contract with Barnes & Noble whereby Barnes & Noble became obligated to reasonably safeguard Plaintiff' and the other Class members' sensitive, non-public, information.

69. Under the implied contract, Barnes & Noble was obligated to not only safeguard customer financial information, but also to provide customers with prompt, adequate notice of any security breach or unauthorized access of said information.

70. Barnes & Noble breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their financial data.

71. Barnes & Noble also breached its implied contract with Plaintiff and the other Class members by failing to provide prompt, adequate notice of the Security Breach and unauthorized access of customer financial information by third-party skimmers.

72. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to loss of their financial information, loss of money and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (and Substantially Similar Laws of the Consumer Fraud States[18]) (on Behalf of the Consumer Fraud Multistate Class)

73. Plaintiff incorporates paragraphs 1-65 as if fully set forth herein.

74. Plaintiff and the other members of the Class were deceived by Barnes & Noble's failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while shopping at Barnes & Noble.

75. Barnes & Noble intended for Plaintiff and the other members of the Class to rely on Barnes & Noble to protect the information furnished to it in connection with their debit and credit card transactions, in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

[18] The Consumer Fraud States were defined at *supra* note 17.

76. Barnes & Noble instead handled Plaintiff and the other Class members' personal information in such manner that it was compromised.

77. Barnes & Noble either willfully ignored its contractual obligations to Visa and other PCI members and failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

78. It was foreseeable that Barnes & Noble's willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

79. Barnes & Noble benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Barnes & Noble saved on the cost of those security measures.

80. Barnes & Noble's fraudulent and deceptive acts and omissions were intended to induce Plaintiff and the other Class members' reliance on Barnes & Noble's deception that their financial information was secure and protected when using debit and credit cards to shop at Barnes & Noble.[19]

81. Barnes & Noble violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff' and the other members' private financial information.

82. Barnes & Noble's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information and failing to promptly notify consumers individually of the Security Breach, constitute separate violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

[19] The consumer protection statutes or interpretive law of the Consumer Fraud States have also either: (a) expressly prohibited omissions of material fact, without regard for reliance on the deception, or (b) have not addressed those issues.

83. Barnes & Noble's conduct constitutes unfair acts or practices as defined in that statute because Barnes & Noble caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

84. Barnes & Noble also violated 815 ILCS 505/2 by failing to immediately notify affected customers of the nature and extent of the Security Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*., which provides:

> Sec. 10. Notice of Breach.
>
> (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

85. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

86. Plaintiff and the other members have suffered injury in fact and actual damages including lost money and property as a result of Barnes & Noble's violations of 815 ILCS 505/2.

87. Plaintiff's and the other Class members' injuries were proximately caused by Barnes & Noble's fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

88. By this conduct, Barnes & Noble violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in her favor and against Barnes & Noble, Inc., as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;

B. Ordering Barnes & Noble to pay for not less than three years of credit card monitoring services for Plaintiff and the other members of the Class;

C. Ordering Barnes & Noble to pay actual damages to Plaintiff and the other members of the Class;

D. Ordering Barnes & Noble to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

E. Ordering Barnes & Noble to pay statutory damages, as provided by the Illinois Consumer Fraud and Deceptive Business Practices Act and other applicable State Consumer Fraud Acts, to Plaintiff and the other members of the Class;

F. Ordering Barnes & Noble to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach in all of its affected stores;

G. Ordering Barnes & Noble to pay attorneys' fees and litigation costs to Plaintiff and the other members of the Class;

H. Ordering Barnes & Noble to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

Date: October 27, 2012

Respectfully submitted,

ELIZABETH NOWAK, individually and on behalf of all others similarly situated

By:_____
One of the Attorneys for Plaintiff
And the Proposed Putative Classes

Joseph J. Siprut
jsiprut@siprut.com
James M. McClintick
jmcclintick@siprut.com
Aleksandra M.S. Vold
avold@siprut.com
SIPRUT PC
17 N. State Street
Suite 1600
Chicago, Illinois 60602
312.236.0000
Fax: 312.948.9212

Adam J. Levitt
levitt@wfafh.com
Edmund S. Aronowitz
aronowitz@whafh.com
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC
55 West Monroe Street, Suite 1111
Chicago, Illinois 60603
312.984.0000
Fax: 312-984-0001

4842-2595-0993, v. 2