Filed: 8/16/2018 9:20 AM
Myla A. Eldridge
Clerk
Marion County, Indiana

STATE OF INDIANA	)	IN THE MARION CIRCUIT/SUPERIOR COURT
	)	
COUNTY OF MARION	)	CAUSE NO. _____

STATE OF INDIANA,	)
	)
Plaintiff,	)
	)
v.	)
	)
EDDIE BAUER LLC,	)
	)
Defendant.	)

COMPLAINT FOR INJUNCTION, CIVIL PENALTIES AND COSTS

Plaintiff, State of Indiana, by Attorney General Curtis T. Hill, Jr. and Deputy Attorneys General Douglas S. Swetnam and Michael A. Eades, petitions the Court, pursuant to the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 ("DCSA"), and the Disclosure of Security Breach Act, Ind. Code § 24-4.9 ("DSBA") for injunctive relief, civil penalties, investigative costs and other relief against Eddie Bauer LLC ("Eddie Bauer" or "Defendant").

PARTIES

1. Plaintiff, State of Indiana, is authorized to bring this action and to seek injunctive and other statutory relief pursuant to Ind. Code § 24-5-0.5-4, and § 24-4.9-4-2.

2. The Attorney General is authorized to bring actions on behalf of the State of Indiana pursuant to Ind. Code § 4-6-3-2.

3. At all times relevant to the allegations herein, Eddie Bauer was and is a limited liability company headquartered and with the principal place of business at 10401 NE 8th Street, Suite 500, Bellevue, Washington 98004 and incorporated in Delaware.

4. At all times relevant, Defendant was registered with the Indiana Secretary of State as a Foreign Limited Liability Company with a business status of "active."

5. Eddie Bauer operates several retail locations in Indiana. By operating retail locations in Indiana, Eddie Bauer was at all times relevant and continues "doing business in Indiana" as the term is defined by Ind. Code § 24-4.9-2-4.

6. Reference in this Complaint to an act of Defendant shall mean that the Defendant performed or authorized its agents, employees, or sub-contractors to perform such act within the scope of its duties, employment, or agency.

JURISDICTION AND VENUE

7. Plaintiff, State of Indiana, is authorized to bring this action and to seek injunctive and other statutory relief pursuant to Ind. Code § 24-5-0.5-4, and § 24-4.9-4-2.

8. The Attorney General is authorized to bring actions on behalf of the State of Indiana pursuant to Ind. Code § 4-6-3-2.

9. At all times relevant to the allegations herein, Defendant was a citizen of Washington and is incorporated in Delaware.

10. At all times relevant to the allegations herein, Defendant operated one retail location in Marion County: 49 West Maryland Street, Indianapolis, Indiana 46204.

11. Defendant was or is involved in consumer transactions in Indiana, as defined by Ind. Code § 24-5-0.5-2.

12. Defendant is subject to an Indiana court pursuant to Ind. Trial R. 4.4(A)(1).

13. Venue is proper in this Court pursuant to Ind. Trial R. 75(A)(4).

FACTS

A. Background.

14. At all times relevant to the allegations herein, Eddie Bauer operated multiple retail locations at which Eddie Bauer sold clothing and general merchandise to tens of thousands of Indiana residents.

15. The transactions involve the sale of a consumer good or service, and therefore are "consumer transactions," as defined by Ind. Code § 24-5-0.5-2(a)(1).

16. By engaging in consumer transactions, Eddie Bauer is a "supplier" as defined by Ind. Code § 24-5-0.5-2(a)(3).

17. Eddie Bauer's retail locations accepted payment cards for purchase of goods and services.

18. When a customer uses a payment card, the transaction involves four primary parties: (1) Eddie Bauer, the merchant; (2) an acquiring bank that has contracted with Eddie Bauer to process payment cards; (3) a card network or payment processor, like Visa or Discover; and (4) the consumer's issuing bank

19. Processing a payment card transaction involves four major steps:

a. *Authorization:* a customer presents a card to make a purchase and then Eddie Bauer requests authorization from the customer's issuing bank.

b. *Clearance:* if the issuer authorizes the transaction, Eddie Bauer completes the sale and forwards a purchase receipt to the acquiring bank.

c. *Settlement:* the acquiring bank pays Eddie Bauer for the purchase and forwards the receipt to the customer's issuing bank.

d. *Post-Settlement:* the customer's issuing bank posts the charge to the customer's payment card.

20. Eddie Bauer accepted payment cards from Visa, MasterCard, Discover, American Express, JCB, and Diner's Club International.

21. Eddie Bauer derived a large portion of its sales to Indiana residents through the use of credit or debit cards. During these sales transactions, Eddie Bauer collected information from Indiana residents, such as the individuals' full names or first initial and last name and the individuals' credit card numbers, debit card numbers, or other financial account numbers (collectively, "Data").

22. The Data was "Personal Information," as defined by Ind. Code § 24-4.9-2-10 ("an individual's first and last name" and "credit card number" or "debit card number in combination with a security code.").

23. Eddie Bauer was a "Data Base Owner" as the term is defined in Ind. Code § 24-4.9-2-3 ("means a person that owns or licenses computerized data that includes personal information.").

24. The Data was, at some time, maintained or stored on a computer. The Data was used to process payments for the transactions with Indiana residents.

25. Upon information and belief, Eddie Bauer displayed to Indiana residents the logos of the major payment card brands Eddie Bauer accepted, explicitly or implicitly representing to consumers Eddie Bauer complied with payment card security rules.

26. Upon information and belief, Eddie Bauer displayed to Indiana residents the logos of the major payment card brands Eddie Bauer accepted, but omitted any warning to consumers that it did not follow the payment card security rules.

27. Upon information and belief, Eddie Bauer employees verbally communicated to some number of the customers what payment cards Eddie Bauer accepted.

B. Eddie Bauer's knowledge of its responsibility to be PCI DSS compliant.

28. Companies that accept credit cards and debit cards for payment must implement specific security measures, Payment Card Industry Data Security Standards ("PCI DSS"), as a minimum standard to protect payment information. *PCI Quick Reference Guide*, PCI Security Standards Council (2008), https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf ("The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS").

29. PCI DSS contains a list of twelve information security mandates. The basic requirements are: (1) Install and maintain a firewall configuration to protect cardholder data; (2) Do not use vendor-supplied defaults for system passwords and other security parameters; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (7) Restrict access to cardholder data by business need to know; (8) Identify and authenticate access to system components; (9) Restrict physical access to cardholder data; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel. *Id.*

30. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

31. Eddie Bauer is, and at all relevant times has been, aware that the Data was highly sensitive.

32. Eddie Bauer is, and at all relevant times has been, aware of the importance of safeguarding the Data and of the foreseeable consequences that would occur if its data security systems were breached.

33. On Eddie Bauer's website, the Privacy & Security statements declares that "we firmly believe in your privacy and the security of your personal information. We are committed to using any information you give us in a responsible manner."[1] Eddie Bauer also states that "We have appropriate security measures in place to protect against the loss, misuse or alteration of information that we have collected from you so you can feel comfortable and secure when shopping."[2]

34. Before January 1, 2016, Eddie Bauer was aware of the threat of a data breach given the prior high-profile breaches that occurred with similar Point of Sale ("POS") malware at Target, Home Depot, Wendy's and others. Visa warned merchants, including Eddie Bauer, as early as August 2013 of Random Access Memory ("RAM") scraping malware targeting POS systems.[3] In February 2014, Visa again warned Eddie Bauer and other merchants of the increased risks posed by RAM scraping malware.[4]

35. Eddie Bauer received additional warnings from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted

[1] *Privacy & Security*, Eddie Bauer (Edited on Jan. 26, 2016), http://www.eddiebauer.com/company-info/company-info-privacy-and-security.jsp.
[2] *Id.*
[3] *Data Security Alert, Visa, Retail Merchants Targeted by Memory-Parsing Malware*, Visa (August 2013), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf (last visited May 21, 2018).
[4] *Data Security Alert, Visa, Retail Merchants Targeted by Memory-Parsing Malware*, Visa (Feb. 2014), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf (last visited May, 21 2018).

retailers to the threat of RAM scraping malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of RAM scraping malware.[5]

36. In August 2015, Eddie Bauer hired Mandiant, a forensic investigation company, to assess the Defendant's internal security vulnerabilities. Mandiant found several "high risk" vulnerabilities, including: 1) Eddie Bauer had servers with Windows 2000 and Windows 2003 operating systems, both of which were no longer supported by Microsoft; 2) Eddie Bauer's network was not properly segmented; 3) Eddie Bauer's POS systems were vulnerable to the type of RAM scraping malware that had been involved in the high profile Data breaches at Target, The Home Depot, Wendy's and P.F. Chang's, and 4) Eddie Bauer permitted unrestricted domain administrator accounts, which allowed administrators to be logged into several servers at once, with clear text passwords remaining in memory, including the administrative accounts of Admin_ppekal and Admin_schang, whom Mandiant specifically identified.

C. Eddie Bauer's PCI DSS failings.

37. Upon information and belief, prior to the Data breach, Eddie Bauer did not maintain a system of accountability for data security, including Eddie Bauer's senior management having knowledge of the security deficiencies that left the Data at risk.

38. At all times relevant, Eddie Bauer had a policy for "vulnerability scanning processes," which required, "Vulnerabilities ranked as critical, high or PCI fail must be remediated within 30 days of discovery."[6]

[5] *See Alert (TA14-212A): Backoff Point-of-Sale Malware*, United States Computer Emergency Readiness Team (Aug. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A (last visited May 21, 2018).

[6] Eddie Bauer, "Vulnerability Scanning Processes," June 2014, p.3.

39. Upon information and belief, Eddie Bauer failed to make timely upgrades and updates to their POS systems.

40. Upon information and belief, Eddie Bauer refused to implement recommended security measures.

41. Despite being informed of the "high risk" vulnerabilities discovered by Mandiant, Eddie Bauer was unwilling to remediate its known vulnerability to RAM scraping malware, choosing instead to "consider" implementing "end to end encryption" only when its legacy order management systems were decommissioned.

42. Upon information and belief, Eddie Bauer did not, in fact, implement point-to-point encryption prior to January 1, 2016, which would have addressed the RAM scraping malware threat.

43. Upon information and belief, Eddie Bauer did not implement tokenization, which would have addressed the RAM scraping malware threat.

44. Upon information and belief, Eddie Bauer did not implement Europay Mastercard® Visa® ("EMV") technology, which would have addressed the RAM scraping malware threat.

45. During the relevant time period, Eddie Bauer was not compliant with PCI DSS requirements 1.2.1 and 1.3.4 that stipulate inbound and outbound traffic are restricted to that which is necessary for the PCI environment.[7]

46. During the relevant time period, Eddie Bauer was not compliant with PCI DSS requirement 6.4.1 that stipulates development and production environments are separated. Eddie Bauer's PCI-related development server was able to interact with the production environment.[8]

[7] Verizon, "Eddie Bauer LLC: Final PFI Report," October 16, 2016, Version 1.1, p. 43.
[8] *Id*. p.44.

47. During the relevant time period, Eddie Bauer was not compliant with PCI DSS requirement 10.2.1 that stipulates that audit trails and logs must be implemented for all individual user access to the PCI environment. Eddie Bauer had insufficient audit trails and logs.[9]

D. Eddie Bauer's PCI DSS failings led to the data breaches.

48. As early as December 24, 2015, Eddie Bauer's network was breached by an unauthorized individual ("intruder"), who established a connection to an external IP address.[10]

49. Beginning on January 1, 2016, the intruder installed RAM scraping malware ("Malware") on 947 POS systems located in 337 of Eddie Bauer's retail locations. The Malware collected the Data and transmitted it to an external IP address (es) and domain(s), and then deleted the record and the results of his activities.

50. The intruder was able to breach Eddie Bauer's Credit Data Environment ("CDE") by leveraging compromised Eddie Bauer user accounts, including two administrator accounts that were specifically identified as vulnerable by Mandiant in August 2015, as described above.

51. During the time period of January 1, 2016 to July 17, 2016, Malware was installed on 947 POS systems, across 337 Eddie Bauer retail locations, including six Indiana locations: Carmel, Edinburgh, Fort Wayne, Granger, Indianapolis Circle Center Mall, and Indianapolis Castleton Square Mall.

52. On July 5, 2016, Brian Krebs, of Krebs on Security, a credible resource in the data privacy industry, alerted Eddie Bauer of a likely breach of its systems. Eddie Bauer responded to Krebs, stating that it "was grateful for the outreach, but that it hadn't heard any fraud complaints from banks or from the credit card associations."[11]

---

[9] *Id*. p. 45.
[10] *Id*. pp. 13-14.
[11] Brian Krebs, *Malware Infected All Eddie Bauer Stores in U.S., Canada*, Krebs on Security (Aug. 18, 2016), https://krebsonsecurity.com/2016/08/malware-infected-all-eddie-bauer-stores-in-u-s-canada/.

53. On July 15, 2016, Eddie Bauer reported to the Federal Bureau of Investigation that it had identified Malware operating on its POS systems.

54. On July 17, 2016, twelve days after the credible Krebs breach notice and two days after its report to the FBI, Eddie Bauer finally removed the Malware from its POS systems.

55. Between July 5, 2016 and July 17, 2016, Eddie Bauer continued to accept payment cards at each of its stores and each of its POS systems, despite knowing its systems were compromised.

56. Between July 15, 2016 and July 17, 2016, Eddie Bauer continued to accept payment cards for processing with its POS systems, despite knowing its systems were infected with Malware.

57. Eddie Bauer knew that by exposing customer Data to its infected systems, customers may become victims of identity theft and fraud.

E. Post Breach.

58. Upon information and belief, during the relevant time period ("January 1, 2016 to July 17, 2016), the RAM scraping Malware collected Data from 2,192,422 individuals, including 22,575 Indiana residents.

59. On August 1, 2016, Verizon, after entering into a contract with Eddie Bauer, began its independent PCI Forensic Investigation ("PFI"), as required by Payment Card Industry rules.[12]

60. On August 18, 2016, Eddie Bauer released a press release, saying that it found malware on POS systems at approximately 370 stores.

61. On August 18, 2016, Eddie Bauer began sending notices to the affected Indiana residents.

[12] Verizon, p. 7.

62. On August 18, 2016, Eddie Bauer published a press release on the data breach.

63. On August 18, 2016, Eddie Bauer alerted the Indiana Attorney General's Office of the Data breach indicating the breach affected a total of 2,192,422 people, including 22,575 Indiana residents.

64. Between July 5, 2016 and August 18, 2016, Eddie Bauer denied the existence of the data breach, thus concealing the breach from Indiana residents and the Attorney General.

65. It was not until August 18, 2016 that Indiana residents and the Attorney General had notice of the breach and its extent.

66. In the August 18, 2016 press release, Mike Egeck, Chief Executive Officer of Eddie Bauer, stated, "The security of our customers' information is a top priority for Eddie Bauer."

67. Customers who used payment cards at Eddie Bauer during the breach may have suffered "1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at [merchant] that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692 (7th Cir. 2015).

68. As a result of the Eddie Bauer breach, hundreds of thousands of payment cards were exposed, and the financial fraud committed by identity thieves with those breached cards was in excess of Three Million Dollars.[13]

69. At least two Indiana financial institutions, Interra Credit Union, Main Office 300 West Lincoln Avenue Goshen, IN 46526, and Forum Credit Union, 11313 USA Parkway Fishers, IN 46037, suffered financial losses as a result of fraudulent transactions resulting from payment cards

[13] Visa, "Event Qualification Summary Under the Visa Global Compromised Account Recovery (GCAR) Program," June 5, 2018 p.14.

exposed by the Eddie Bauer data breach. Interra alone estimates its losses at approximately Sixteen Thousand Dollars ($16,000.00).

70. Had Eddie Bauer implemented proper data security measures and promptly remedied the known "high risk" deficiencies in its IT systems, it could have prevented the data breach because virtually all data breaches are preventable. For its annual report, the Online Trust Alliance, a non-profit organization committed to enhancing trust online, estimate that 93% of the breaches occurring in 2017 were preventable.[14]

COUNT I: INJUNCTION FOR VIOLATION OF THE DCSA

71. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

72. The transactions referenced above involve the sale of a consumer good or service, therefore, the transactions are "consumer transactions," as defined by Ind. Code § 24-5-0.5-2(a)(1).

73. By engaging in consumer transactions, Eddie Bauer is a "supplier" as defined by Ind. Code § 24-5-0.5-2(a)(3).

74. The DCSA prohibits a supplier from committing "an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." Ind. Code § 24-5-0.5-3(a).

75. By displaying the logos of the payment cards it accepted, Eddie Bauer explicitly or implicitly represented that it followed the rules for payment cards.

[14] *Online Trust Alliance Reports Doubling of Cyber Incidents in 2017*, OTA (Jan. 25, 2018), https://otalliance.org/news-events/press-releases/online-trust-alliance-reports-doubling-cyber-incidents-2017-0.

76. By accepting payment cards, Eddie Bauer misrepresented that it was PCI DSS compliant and omitted disclosing its lack of PCI DSS compliancy.

77. Each of the transactions by the 22,575 Indiana residents represents a customer using a payment card in one of the stores in which Eddie Bauer failed to implement expected and standard security measures and failed to comply with PCI DSS requirements.

78. Each of the transactions by the 22,575 Indiana residents represents a customer who had a reasonable expectation that Eddie Bauer was complying with the industry standards and requirements, *e.g.* PCI DSS compliance, set by payment processing networks, like Visa, MasterCard, Discover, and American Express.

79. By accepting payment cards, Eddie Bauer explicitly and implicitly misrepresented to its customers that Eddie Bauer was PCI DSS compliant, when it in fact was not.

80. When accepting payment cards, Eddie Bauer omitted information about its lack of reasonable security measures, such as the "high risk" vulnerabilities identified by Mandiant prior to the breach.

81. Eddie Bauer knew the importance of its customers' personal data.

82. Eddie Bauer knew that it needed to be PCI DSS compliant and that it was solely responsible for said compliancy.

83. Eddie Bauer knowingly committed an unfair, abusive, or deceptive act when it accepted payment card transactions during the relevant time period.

84. When determining whether certain acts are unfair, consideration includes whether the acts offend public policy, are unethical, or cause substantial injury to consumers.

85. First, the DSBA requires Eddie Bauer to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from

unlawful use or disclosure any personal information of Indiana residents collected or maintained by [Eddie Bauer]." Ind. Code § 24-4.9-3-3.5(c).

86. The payment card industry's standard, PCI DSS, is the reasonable security standard. It is antithetical to the public policy of the DSBA for Eddie Bauer to conduct consumer transactions outside of the PCI DSS framework.

87. Second, it's unethical for Eddie Bauer to put its customers' payment card information at risk when Eddie Bauer knew that the information was not adequately protected and, from July 5, 2016 until July 15, 2016, knew that the information was imminently at risk of being breached, and between July 15, 2016 until July 17, 2016, knew the information was being exposed to active Malware.

88. Finally, the costs incurred by all of the customers whose payment information was affected by the data breaches constitute substantial injuries. From January 1, 2016 to July 17, 2016, there were at least 22,575 separate transactions at Eddie Bauer's Indiana locations.

89. Affected consumers spent time and money to monitor and repair their financial accounts and statements for fraudulent charges and identity theft. *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966-67 (7th Cir. 2016) (holding that injuries such as time and money spent by customers to protect against future identity theft or fraudulent charges, mitigation expenses, are "actual injuries" when harm is imminent, such as when a data breach has already occurred). *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015).

90. In addition, as a result of the Eddie Bauer breach, hundreds of thousands of payment cards were exposed, and the financial fraud committed with those breached cards was

in excess of Three Million Dollars,[15] including the financial fraud suffered by Indiana financial institutions, including but not limited to Interra Credit Union and Forum Credit Union.

91. From January 1, 2016 to July 17, 2016, each of the transactions entered by the 22,575 Indiana residents represents an unfair act, omission, and misrepresentation which constitutes a deceptive act committed by Eddie Bauer in violation of the DCSA, Ind. Code § 24-5-0.5-3(b)(7).

92. Accordingly, Eddie Bauer is subject to the remedies provided under Ind. Code § 24-5-0.5-4(c), including, without limitation, injunction, restitution, reimbursement of costs of the investigation and prosecution of the action.

COUNT II: DEFENDANT KNOWINGLY VIOLATED THE DCSA AND SHOULD BE ASSESSED CIVIL PENALTIES

93. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

94. The DCSA prohibits a supplier from committing "an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." Ind. Code § 24-5-0.5-3(a).

95. Plaintiff may seek a civil penalty of up to $5,000 per violation. Ind. Code § 24-5-0.5-4(g) if the Defendant "has knowingly violated section 3 . . . of this chapter. . ."

96. The purpose and policy for the DCSA is to "protect consumers from suppliers who commit deceptive and unconscionable sales acts" and "encourage the development of fair

[15] Visa, p.14..

consumer sales practices." Ind. Code § 24-5-0.5-1. As such, the DCSA should be "liberally construed and applied to promote its purposes and policies." *Id.*

97. Each of the transactions the 22,575 Indiana residents entered with Eddie Bauer during the relevant time period represents a customer using a payment card in one of the stores in which Eddie Bauer failed to implement expected and standard security measures and failed to comply with PCI DSS requirements.

98. Each of the transactions the 22,575 Indiana residents entered with Eddie Bauer during the relevant time period represents a customer who had a reasonable expectation that Eddie Bauer was complying with the industry standards and requirements, *e.g.* PCI DSS compliance, set by payment processing networks, like Visa, MasterCard, Discover, and American Express.

99. By accepting payment cards, Eddie Bauer explicitly and implicitly misrepresented to each of those customers that Eddie Bauer was PCI DSS compliant, when it in fact was not.

100. When accepting payment cards, Eddie Bauer omitted information about its lack of reasonable security measures, such as the "high risk" vulnerabilities identified by Mandiant.

101. Eddie Bauer knowingly committed an unfair, abusive, or deceptive act when it accepted payment card transactions during the relevant time period.

102. Eddie Bauer knew the importance of its customers' personal data.

103. Eddie Bauer knew that it needed to be PCI DSS compliant and that it was solely responsible for said compliancy.

104. Eddie Bauer knew that each store needed to be PCI DSS compliant.

105. When determining whether certain acts are unfair, consideration includes whether the acts offend public policy, are unethical, or cause substantial injury to consumers.

106. First, the DSBA requires Eddie Bauer to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by [Eddie Bauer]." Ind. Code § 24-4.9-3-3.5(c).

107. The payment card industry's standard, PCI DSS, is the reasonable security standard. It is antithetical to the public policy of the DSBA for Eddie Bauer to conduct consumer transactions outside of the PCI DSS framework.

108. Second, it's unethical for Eddie Bauer to put its customers' payment card information at risk when Eddie Bauer knew that the information was not adequately protected and, from July 5, 2016 until July 15, 2016, knew that the information was imminently at risk of being breached, and between July 15, 2016 until July 17, 2016, knew the information was being exposed to active Malware.

109. Finally, the costs incurred by all of the customers whose payment information was affected by the data breaches constitute substantial injuries. From January 1, 2016 to July 17, 2016, there were at least 22,575 separate transactions by Indiana residents at Eddie Bauer's stores.

110. Affected consumers spent time and money to monitor and repair their financial accounts and statements for fraudulent charges and identity theft. *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966-67 (7th Cir. 2016) (holding that injuries such as time and money spent by customers to protect against future identity theft or fraudulent charges, mitigation expenses, are "actual injuries" when harm is imminent, such as when a data breach has already occurred). *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015).

111. In addition, as a result of the Eddie Bauer breach, hundreds of thousands of payment cards were exposed, and the financial fraud committed with those breached cards was in excess of Three Million Dollars[16], including the financial fraud suffered by Indiana financial institutions Interra Credit Union, Forum Credit Union and others.

112. Accordingly, Plaintiff may seek a civil penalty of up to $5,000 per knowing violation. Ind. Code § 24-5-0.5-4(g).

COUNT III: CIVIL PENALTIES FOR INCURABLE VIOLATION OF THE DCSA

113. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

114. An "Incurable deceptive act" means a deceptive act done "as part of a scheme, artifice, or device with intent to defraud or mislead." Ind. Code § 24-5-0.5-2(a)(8).

115. On July 5, 2016, Eddie Bauer was alerted by a reputable source that its system had been compromised.

116. From July 5, 2016 until July 17, 2016, Eddie Bauer knowingly continued to accept payment cards for consumer transactions, while knowing its POS systems were compromised.

117. From July 15, 2016 until July 17, 2016, Eddie Bauer continued to accept payment cards for consumer transactions, while it knew each of its POS systems was actively infected with Malware.

118. From July 5, 2016 until July 17, 2016, Eddie Bauer explicitly and implicitly misrepresented that its payment card system was secure when it knew it was not.

[16] Visa, p.1

119. From July 5, 2016 until July 17, 2016 Eddie Bauer misled Indiana residents who used a payment card at one of Eddie Bauer's locations by omitting to disclose the ongoing breach.

120. From July 15, 2016 until July 17 2016, Eddie Bauer misled Indiana residents when it omitted a disclosure to consumers that its payment systems were infected with malware and that data compromise was imminent.

121. Eddie Bauer created a scheme that prioritized sales over notification and data security.

122. For each transaction that occurred involving Indiana residents from July 5, 2016 to July 17, 2016, Eddie Bauer took advantage of each customer's reliance on Eddie Bauer to be PCI DSS compliant.

123. For each transaction that occurred involving Indiana residents from July 5, 2016 to July 17, 2016, Eddie Bauer took advantage of each customer's reliance on Eddie Bauer to protect his personal information.

124. For each transaction that occurred involving Indiana residents from July 5, 2016 to July 17, 2016, each customer was misled into making a transaction that he likely would not have entered if Eddie Bauer had disclosed the true state of its payment systems.

125. Accordingly, Eddie Bauer is subject to the penalties provided under Ind. Code § 24-5-0.5-8. Any person "who commits an incurable deceptive act is subject to a civil penalty . . . of not more than five hundred dollars ($500) for each violation."

COUNT IV: DEFENDANT VIOLATED THE NOTIFICATION PROVISION OF THE DSBA

126. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

127. Eddie Bauer was required to disclose the Data breach to affected Indiana residents after it discovered or was notified of the Data breach "without unreasonable delay," as required by Ind. Code § 24-4.9-3-1(a).

128. The 44 day delay before notifying Indiana residents was not made to restore the integrity of the computer system, to discover the scope of the breach, or in response to law enforcement. Thus, the delay of 44 days was unreasonable. Ind. Code § 24-4.9-3-3(a).

129. By failing to disclose a breach of the security of data in accordance with Ind. Code § 24-4.9-3-3, the Defendant committed a deceptive act that is actionable by the Attorney General under Ind. Code § 24-4.9-4-1.

130. Pursuant to Ind. Code § 24-4.9-4-2, the Attorney General may bring an action to enjoin future violations of Ind. Code § 24-4.9-3, seek a civil penalty up to $150,000, and obtain the costs of investigating and maintaining the action.

COUNT V: DEFENDANT VIOLATED THE ATTORNEY GENERAL NOTIFICATION PROVISION OF THE DSBA

131. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

132. Eddie Bauer was required to disclose the Data breach to the Attorney General after it discovered or was notified of the Data breach "without unreasonable delay," as required by Ind. Code § 24-4.9-3-1(c).

133. The 44 day delay in notification to the Attorney General was not made to restore the integrity of the computer system, to discover the scope of the breach, or in response to law enforcement. Thus, the delay of 44 days was unreasonable. Ind. Code § 24-4.9-3-3(a).

134. By failing to disclose a breach of the security of data in accordance with Ind. Code § 24-4.9-3-3, the Defendant committed a deceptive act that is actionable by the Attorney General under Ind. Code § 24-4.9-4-1.

135. Pursuant to Ind. Code § 24-4.9-4-2, the Attorney General may bring an action to enjoin future violations of Ind. Code § 24-4.9-3, seek a civil penalty up to $150,000, and obtain the costs of investigating and maintaining the action.

COUNT V: DEFENDANT VIOLATED THE CONSUMER REPORTING AGENCIES NOTIFICATION PROVISION OF THE DSBA

136. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

137. Eddie Bauer was required to disclose the Data breach to the consumer reporting agencies, as over 1000 Indiana residents were impacted by the Data breach, without unreasonable delay, as required by Ind. Code § 24-4.9-3-1(b).

138. Upon information and belief, Eddie Bauer has not notified the consumer reporting agencies of the Data breach.

139. By failing to disclose a breach of the security of data in accordance with Ind. Code § 24-4.9-3-3, the Defendant committed a deceptive act that is actionable by the Attorney General under Ind. Code § 24-4.9-4-1.

140. Pursuant to Ind. Code § 24-4.9-4-2, the Attorney General may bring an action to enjoin future violations of Ind. Code § 24-4.9-3, seek a civil penalty up to $150,000, and obtain the costs of investigating and maintaining the action.

COUNT VI: DEFENDANT VIOLATED THE SECURITY PROVISION OF THE DSBA

141. Plaintiff alleges and incorporates by reference the allegations contained in the paragraphs above.

142. Eddie Bauer, as a Data Base Owner, was required under Ind. Code § 24-4.9-3-3.5(c) to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."

143. In August 2015, Mandiant identified multiple "high risk" vulnerabilities in Eddie Bauer's computer systems that risked the exposure of customer data.

144. Despite the above-referenced information, Eddie Bauer failed to implement and maintain reasonable procedures to protect and safeguard the Personal Information of Indiana residents, including taking appropriate corrective action for the "high risk" vulnerabilities Mandiant identified, such as Eddie Bauer's vulnerability to RAM scraping malware.

145. Eddie Bauer failed to implement and maintain reasonable procedures to protect and safeguard the Personal Information of Indiana residents, when it was not compliant with PCI DSS requirements to limit inbound and outbound traffic.

146. Eddie Bauer failed to implement and maintain reasonable procedures to protect and safeguard the Personal Information of Indiana residents in that it was not compliant with the PCI DSS requirement to separate development and production servers for PCI related development.

147. Eddie Bauer failed to implement and maintain reasonable procedures to protect and safeguard the Personal Information of Indiana residents in that it was not compliant with the PCI DSS requirement to have audit trails and logs for all individual user access to the PCI environment.

148. Eddie Bauer failed to implement and maintain reasonable procedures to protect and safeguard the Personal Information of Indiana residents through the use unrestricted domain administrator accounts, including Admin_ppekal and Admin_schang, both of which had been identified by Mandiant in August 2015.

149. Eddie Bauer knew that the unauthorized acquisition of its customers' Personal Information, would lead to identity theft or other related harm to affected Indiana residents, as described in Ind. Code § 24-4.9-3-1(a).

150. Ind. Code § 24-4.9-3-3.5(f) provides that a failure to comply with Ind. Code § 24-4.9-3-3.5(c) in connection with related acts or omissions is one deceptive act, subject to a civil penalty up to $5,000, pursuant to Ind. Code § 24-4.9-3-3.5(e)(2).

RELIEF

WHEREFORE, the Plaintiff, State of Indiana, requests the Court enter judgment against the Defendant, EDDIE BAUER LLC, for the following relief:

a. Permanently enjoin Defendant, their agents, representatives, employees, successors, assigns and any other person acting on behalf of the Defendant from engaging in deceptive acts, specifically:

   i. Conducting business activity in the State of Indiana unless those activities are in full compliance with the Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-1, *et seq.*

b. An injunction to enjoin future violations of Ind. Code § 24-4.9-3, pursuant to Ind. Code § 24-4.9-4-2(1);

c. Impose upon Defendant a civil penalty of up to $5,000 per knowing violation of the DCSA, pursuant to Ind. Code § 24-5-0.5-4(g).

i. Every transaction with an Indiana resident that happened between January 1 and July 17, 2016 was a knowing violation of the DCSA, and thus carries a civil penalty of $5,000. There were at least 22,575 transactions.

ii. In the alternative, every transaction with an Indiana resident that happened between July 5 and July 16, 2016 was a knowing violation of the DCSA, and thus carries a civil penalty of $5,000. On information and belief, there was at least 100 transactions with an Indiana resident during this time period.

d. Civil penalties of up to $500 for each incurable deceptive act, pursuant to Ind. Code § 24-5-0.5-8;

e. Civil penalties in the amount of $150,000, pursuant to Ind. Code § 24-4.9-4-2(2), for the Defendant's unreasonable delay in disclosing or notifying a breach of the security of data to affected Indiana Residents;

f. Civil penalties in the amount of $150,000, pursuant to Ind. Code § 24-4.9-4-2(2), for the Defendant's unreasonable delay in disclosing or notifying a breach of the security of data to the Attorney General;

g. Civil penalties in the amount of $150,000, pursuant to Ind. Code § 24-4.9-4-2(2), for the Defendant's unreasonable delay in disclosing or notifying a breach of the security of data to the consumer reporting agencies;

h. Civil penalties in the amount of $5,000, pursuant to Ind. Code § 24-4.9-3-3.5 (e)(2), for each of the Defendant's failure to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner;

i. Pursuant to Ind. Code § 24-4.9-3-2(3), and Ind. Code § 24-5-0.5-4(c)(4), award the Office of Attorney General its reasonable fees and costs incurred in the investigation and prosecution of this matter; and

j. Award all other just and proper relief.

Respectfully submitted,

Curtis T. Hill Jr.
Attorney General of Indiana
Atty. No. 13999-20

By: /s/ Douglas S. Swetnam
Douglas S. Swetnam, Deputy Attorney General
Atty. No. 15860-49
Office of the Attorney General
302 West Washington Street
IGCS - 5th Floor
Indianapolis, IN 46204
Email: douglas.swetnam@atg.in.gov

By: /s/ Michael A. Eades
Michael Eades, Deputy Attorney General
Atty. No. 31015-49
Office of the Attorney General
302 West Washington Street
IGCS - 5th Floor
Indianapolis, IN 46204Email:
michael.eades@atg.in.gov