UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

VERIDIAN CREDIT UNION, on behalf of itself and a class of similarly situated financial institutions, Plaintiff, v. EDDIE BAUER LLC, Defendant.	NO. **CLASS ACTION COMPLAINT** JURY DEMAND

Plaintiff Veridian Credit Union ("Plaintiff"), through its undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, files this Class Action Complaint against Defendant Eddie Bauer LLC ("Eddie Bauer" or "Defendant") and states the following:

INTRODUCTION

1. This is a class action on behalf of credit unions, banks, and other financial institutions that suffered injury as a result of a security breach from or around January 2, 2016 to July 17, 2016[1], which compromised the names, credit and debit card numbers, card expiration dates, card verification values ("CVVs"), and other credit and debit card information (collectively, "Payment Card Data") of customers at approximately 350 American and

[1] To date, the Eddie Bauer Data Breach has been confirmed to have run through July 17, 2016. It is entirely possible that the Eddie Bauer Data Breach ran past this date, which will be confirmed through discovery in this litigation.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Canadian locations of Defendant Eddie Bauer's stores (hereinafter, the "Eddie Bauer Data Breach").

2. The Eddie Bauer Data Breach forced Plaintiff and other financial institutions to take one or more of the following actions: (a) cancel or reissue any credit and debit cards affected by the Eddie Bauer Data Breach; (b) close and/or open or reopen any deposit, transaction, checking, or other accounts affected by the Eddie Bauer Data Breach; (c) refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Eddie Bauer Data Breach; (d) respond to a higher volume of cardholder complaints, confusion, and concern; (e) increase fraud monitoring efforts; and/or (f) other lost revenues as a result of the breach.

3. As alleged herein, the injuries to Plaintiff and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for customer information, including credit and debit card data and personally identifying information. Defendant failed to take steps to employ adequate security measures despite well-publicized data breaches at large national retail and restaurant chains in recent months, including Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Wendy's, Dairy Queen, Noodles, and Kmart.

4. The failure of Defendant to adequately secure its data networks was particularly inexcusable given the fact that the infiltration underlying the Eddie Bauer Data Breach involved mostly the same techniques as those used in major data breaches in the preceding months and years, including those at other major retailers like Target, Home Depot, and Kmart. Nevertheless, despite having knowledge that such data breaches were occurring throughout the retail industry, Defendant failed to properly protect sensitive payment card information.

5. The data breach was the inevitable result of Eddie Bauer's inadequate data security measures and approach to data security. Despite the well-publicized and ever-growing threat of cyber breaches involving payment card networks and systems, Eddie Bauer

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

systematically failed to ensure that it maintained adequate data security measures, failed to implement best practices, failed to upgrade security systems, and failed to comply with industry standards by allowing its computer and point of sale systems to be hacked causing financial institutions' payment card and customer information to be stolen. Eddie Bauer's data security deficiencies were so significant that hackers were able to install malware and remain undetected for months, until outside parties notified Eddie Bauer that its computer and point of sale systems may have been breached as a result of the identification of fraudulent transactions that had taken place after the hackers had used or sold customer data.

6. Defendant also failed to mitigate the damage of a potential data breach by failing to implement chip-based card technology, otherwise known as EMV technology. EMV – which stands for Europay, MasterCard, and Visa – is a global standard for cards equipped with computer chips and technology used to authenticate chip card transactions. While Visa implemented minimum EMV Chip Card and Terminal Requirements in October 2015, at the time of the Eddie Bauer Data Breach, Defendant had not fully implemented EMV technology in its stores, and thus, left all of the information on the magnetic stripe of cards used in its retail locations vulnerable to theft in a way it has been repeatedly warned about.

7. In addition to failing to prevent the intrusion in the first instance and failing to implement required data security measures that would have limited its ability to affect cardholders and the financial institutions from which their cards came, Defendant exacerbated injury by failing to notify customers of the infiltration for a period of at least six weeks from being first informed by a third party that the Eddie Bauer Data Breach had occurred, after letting the breach itself go undetected for over six months. Eddie Bauer store payment data systems were infected with a form of malware of which Defendant was unaware until July or even August 2016. Therefore, the volume of data stolen was much greater than it would have

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

been had Defendant maintained sufficient malware monitoring to identify and eliminate the breach as it was occurring.

8. As a direct and proximate consequence of Defendant's negligence, vast amounts of customer information were stolen from the Eddie Bauer computer network. Though an investigation is still ongoing, it appears that hundreds of thousands or even millions of Defendant's customers at approximately 350 American and Canadian locations have had their credit and debit numbers compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identity theft, and have otherwise suffered damages. Moreover, Plaintiff and members of the Class have incurred, and have a certainly impending risk of incurring in the future, significant costs associated with having to respond to the breach in one or more of the ways: notifying their customers of issues related to the Eddie Bauer Data Breach, closing out and opening new customer accounts, reissuing customers' cards, and/or refunding customers' losses resulting from the unauthorized use of their accounts.

9. Plaintiff and the members of the Class seek to recover damages caused by Defendant's negligence, negligence *per se*, violation of RCW 19.255.020, violation of RCW Ch. 19.86, and for declaratory and injunctive relief.

PARTIES

10. Plaintiff Veridian Credit Union ("Veridian" or "Plaintiff") is an Iowa-chartered credit union with its principal place of business located in Waterloo, Iowa. As a result of the Eddie Bauer Data Breach, Plaintiff Veridian has suffered and is subject to a certainly impending risk of suffering, injury in one or more of the following ways: costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and other lost revenues.

11. Defendant Eddie Bauer LLC ("Eddie Bauer") is headquartered at 10401 NE 8th Street, Suite 500, Bellevue, Washington 98004. According to its website, "Eddie Bauer offers premium-quality clothing, accessories and gear for men and women that complement today's

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

modern outdoor lifestyle." Eddie Bauer operates approximately 370 stores throughout the United States and Canada.[2]

JURISDICTION AND VENUE

12. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. §1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class, defined below, many of which are citizens of a different state than Defendant. Defendant Eddie Bauer is a citizen of Washington, where its principal place of business is located.

13. The Western District of Washington has personal jurisdiction over Defendant because Defendant is found within this District and conducts substantial business in this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because Defendant resides in this judicial district, regularly transacts business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

FACTUAL BACKGROUND

A. Background on Electronic Debit and Credit Card Transactions and Requirements for Securing Data

15. Plaintiff and the members of the Class are financial institutions that issue payment cards[3] to their customers.

16. Eddie Bauer stores accept customer payment cards for the purchase of goods and services. At the point of sale ("POS"), these cards are swiped on a POS terminal and either a personal identification number (or some other confirmation number) is entered or a receipt is signed to finish the transaction on behalf of the customer.

[2] http://www.eddiebauer.com/company-info/company-info-about-us.jsp (last visited on Mar. 7, 2017)).

[3] These cards include, for example, debit or credit cards branded with the Visa or MasterCard logo.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

17. It is well known that customer Payment Card Data is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and restaurants nationwide, including Home Depot, Target, Kmart, Wendy's, P.F. Chang's, Neiman Marcus, and many others. Indeed, Eddie Bauer should have been especially aware of the threat posed by data breaches since in April 2011, Eddie Bauer customers were warned that hackers may have obtained access to email addresses and other personal information because of a breach at Epsilon. Despite widespread publicity and industry alerts regarding these other notable data breaches, Eddie Bauer failed to take reasonable steps to adequately protect its computer systems from being breached.

18. A large portion of sales at Eddie Bauer's stores are made to customers using credit or debit cards. A basic description of the various steps necessary to execute a credit/debit card transaction is as follows: (1) after the credit/debit card is swiped, the merchant (*e.g.*, Eddie Bauer) uses one of several payment processing networks (*e.g.*, Visa or MasterCard) to transmit a request for authorization to the institution that issued the payment card (*e.g.*, Plaintiff); (2) the issuing institution authorizes the payment and the merchant electronically forwards a receipt of the transaction to another financial institution, known as the "acquiring bank," which contracts with the merchant to process credit and debit card transactions on the merchant's behalf; (3) the acquiring bank forwards the funds to the merchant to satisfy the transaction and is then reimbursed by the issuing financial institution (*e.g.*, Plaintiff); and (4) finally, the issuing institution posts the debit or credit transaction to its customer's account.

19. Eddie Bauer is, and at all relevant times has been, aware that the Payment Card Data it maintains is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

20. Eddie Bauer is, and at all relevant times has been, aware of the importance of safeguarding its customers' Payment Card Data and of the foreseeable consequences that would

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

occur if its data security systems were breached, specifically including the significant costs that would be imposed on issuers, such as the Plaintiff, members of the Class, and others.

21. Given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, it is unsurprising that financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure consumers' valuable data is protected.

22. The Payment Card Industry Data Security Standards ("PCI DSS") is a list of 12 information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted and requires merchants like Defendant to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

23. The 12 requirements of the PCI DSS are:

Build and Maintain a Secure Network

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

Protect Cardholder Data

3) Protect stored cardholder data

4) Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5) Protect all systems against malware and regularly update anti-virus software or programs

6) Develop and maintain secure systems and applications

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

10) Track and monitor all access to network resources and cardholder data

11) Regularly test security systems and processes

Maintain an Information Security Policy

12) Maintain a policy that addresses information security for all personnel.[4]

24. Furthermore, PCI DSS 3.1 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates. Defendant was at all times fully aware of its data protection obligations for Eddie Bauer stores in light of their participation in the payment card processing networks and their daily collection and transmission of tens of thousands of sets of Payment Card Data.

25. Furthermore, Defendant knew that because they accepted payment cards at Eddie Bauer stores containing sensitive financial information, customers and financial institutions, such as Plaintiff, were entitled to, and did, rely on Defendant to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

26. In addition, the payment card industry also set rules requiring all businesses to upgrade to new card readers that accept EMV chips. EMV chip technology uses embedded computer chips instead of magnetic stripes to store Payment Card Data. Unlike magnetic stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used

[4] PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2*, at 9 (May 2016), https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1472840893444 (last visited Mar. 7, 2017).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the thieves, making it much more difficult for criminals to profit from what is stolen.

27. The payment card industry (MasterCard, Visa, Discover, and American Express) set a deadline of October 1, 2015, for businesses to transition their systems from magnetic stripe to EMV technology. Eddie Bauer did not meet that deadline.

28. Under Card Operating Regulations, businesses accepting payment cards, but not meeting the October 1, 2015 deadline, agree to be liable for damages resulting from any data breaches.

29. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by §5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. §45.

30. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

31. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

such risks.[5]

32. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses in regard to their data security obligations.

B. The Eddie Bauer Data Breach: the Result of Lax Security Standards

33. On July 5, 2016, Brian Krebs, of KrebsOnSecurity, a leading information security investigator, reached out to Eddie Bauer after hearing from several sources who work in fighting fraud at American financial institutions of a possible breach at Eddie Bauer retail locations. All of those sources said they had identified a pattern of fraud on customer cards that had one thing in common: they were all used at Eddie Bauer's American retail locations. A spokesperson for Eddie Bauer at the time said that Defendant was grateful for the outreach, but that Eddie Bauer had not received any fraud complaints from banks or credit card associations.

34. Recognizing the impact the Eddie Bauer Data Breach would have on financial institutions like Plaintiff and other members of the Class, Eddie Bauer stated that "[i]f a customer believes his or her payment card may have been affected, the customer should immediately contact their bank or card issuer."

35. Despite notice from Krebs on Security in early July 2016, Eddie Bauer did not officially confirm the Eddie Bauer Data Breach until it released a statement on August 18, 2016, over six weeks later, saying that Defendant had found malware on its registers at approximately 350 stores, and that there was reason to believe that credit and debit cards used at these stores between January 2 and July 17, 2016 "may have been compromised."

36. In a communication to KrebsOnSecurity, Eddie Bauer said that they had been working with the U.S. Federal Bureau of Investigation and an outside computer forensics firm,

[5] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Nov. 2011), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 7, 2017).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and they had detected and removed card-stealing malware from cash registers at ***all*** of Eddie Bauer's locations in the United States and Canada.

37. Eddie Bauer further stated that it believed the malware was capable of capturing credit and debit card information from customer transactions made at ***all*** Eddie Bauer stores in the United States and Canada from January 2, 2016 to July 17, 2016.

38. Eddie Bauer offered to its customers whose credit and debit card information were potentially captured by the malware, 12 months of identity protection services from Kroll, a global leader in risk mitigation and response.

39. Eddie Bauer setup a website for customers whose payment card information may have been accessed during the Eddie Bauer Data Breach, http://cardnotification.kroll.com/. On this website, Eddie Bauer stated that "unauthorized parties [were able] to access payment card account information." Specifically, these unauthorized parties took "cardholder name, payment card number, security code and expiration date" information. However, despite these facts, Eddie Bauer has not offered Financial Institutions any compensation for the fraud losses or reissuance costs associated with credit and debit cards that were potentially captured by the malware.

40. On August 18, 2016, the Company issued a press release regarding the breach:

"We have been working closely with the FBI, cyber security experts, and payment card organizations, and want to assure our customers that we have fully identified and contained the incident and that no customers will be responsible for any fraudulent charges to their accounts. In addition, we've taken steps to strengthen the security of our point of sale systems to prevent this from happening in the future."

41. The press release went on to state that it was working with payment card networks to identify and monitor the breach: "Eddie Bauer has notified payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used during the timeframe in which cards may have been compromised."

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

42. Additionally, on August 18, 2016, the Company's CEO, Mike Egeck issued an open letter acknowledging that credit and debit card data had been compromised similar to many other merchants throughout the United States:

> Unfortunately, malware intrusions like this are all too common in the world that we live in today. In fact, ***we learned that the malware found on our systems was part of a sophisticated attack directed at multiple restaurants, hotels, and retailers, including Eddie Bauer***. We are conducting a comprehensive review of our IT systems to incorporate recommended security measures in order to strengthen them and prevent this from happening again. We have been working closely with payment card organizations and customers will not be responsible for any fraudulent charges to their accounts. We also have been working with the FBI to identify the perpetrators and provide whatever cooperation is necessary to hold them accountable.[6]

43. Even now, many months after the Eddie Bauer Data Breach ended, the website still says that Eddie Bauer has only "started the process of notifying customers whom we have confirmed may have been affected," so the impact of the Eddie Bauer Data Breach is likely to continue to grow.

44. The deficiencies in Eddie Bauer's security system include a lack of elementary security measures that even the most inexperienced IT professional could identify as problematic.

45. Had Eddie Bauer remedied the deficiencies in its IT systems, it could have prevented the Eddie Bauer Data Breach because virtually all data breaches are preventable. In fact, the *Online Trust Alliance*, a non-profit organization whose mission is to enhance online trust, user empowerment, and innovation, in its 2014 annual report, estimated that 740 million records were stolen in 2013, and that 89% of data breaches occurring in that year were avoidable.

46. The security flaws outlined above, along with many others, were explicitly highlighted by Visa as early as 2009, when it issued a Data Security Alert describing the threat

[6] http://cardnotification.kroll.com/ (last visited Mar. 7, 2017).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

of RAM scraper malware.[7] The report instructs companies to "secure remote access connectivity," "implement secure network configuration, including egress and ingress filtering to only allow the ports/services necessary to conduct business" (*i.e.*, segregate networks), "actively monitor logs of network components, including intrusion detection systems and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "encrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit" and "work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration." *Id.*

47. In addition to ignoring explicit warnings from Visa, Eddie Bauer's security flaws also run afoul of industry practices and standards. More specifically, the security practices in place at Eddie Bauer are in stark contrast and directly conflict with the Payment Card Industry Data Security Standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

48. Furthermore, mere compliance with the PCI DSS is insufficient to establish reasonably strong data security practices. For example, Georgia Weidman, CTO and founder of Shevirah (a company that tests data security for retailers and other merchants), stated that "Every company that has been spectacularly hacked in the last three years has been PCI complaint . . . . Obviously, based on that evidence, while a good step in the right direction, PCI is not sufficient to protect against breaches."[8]

[7] *Visa Security Alert* (Nov. 6, 2009), http://go.mercurypay.com/go/visa/targeted-hospitality-sector-vulnerabilities-110609.pdf (last visited Mar. 7, 2017).

[8] Sean Michael Kerner, *Eddie Bauer Reveals It Was the Victim of a POS Breach*, EWEEK (Aug. 19, 2016), http://www.eweek.com/security/eddie-bauer-reveals-it-was-the-victim-of-a-pos-breach.html (last visited Mar. 7, 2017).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

49. As a result of industry warnings, industry practice, the PCI DSS, and multiple well-documented data breaches, Defendant was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

50. Defendant was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used to access POS terminals since at least 2011, and specific types of malware, including RAM scraper malware, have been used recently to infiltrate large retailers such as Target, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Defendant was aware that malware is a real threat and is a primary tool of infiltration used by hackers.

51. Defendant received additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of POS malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware, which was updated on August 27, 2014.[9]

52. Despite the fact that Defendant was put on notice of the very real possibility of consumer data theft associated with its security practices and despite the fact that Defendant knew or, at the very least, should have known about the elementary infirmities associated with the Eddie Bauer security systems, it still failed to make necessary changes to its security practices and protocols.

53. Defendant knew that failing to protect customer card data would cause harm to the card-issuing institutions, such as Plaintiff and the Class, because the issuers are financially responsible for fraudulent card activity and must incur significant costs to prevent additional fraud.

[9] *See* United States Computer Emergency Readiness Team, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (Aug. 27, 2014), https://www.us-cert.gov/ncas/alerts/TA14-212A (last visited Mar. 7, 2017).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

54. Indeed, Defendant's public statements to customers after the data breach plainly indicate that Defendant believes that card-issuing institutions should be responsible for fraudulent charges on cardholder accounts resulting from the data breach. Eddie Bauer has made no overtures to the card-issuing institutions that are left to pay for damages as a result of the breach.

55. Defendant, at all times relevant to this action, had a duty to Plaintiff and members of the Class to: (a) properly secure payment card magnetic stripe information at the point of sale and on Defendant's internal networks; (b) encrypt Payment Card Data using industry standard methods; (c) use and deploy up to date EMV technology properly; (d) use available technology to defend its POS terminals from well-known methods of invasion; and (e) act reasonably to prevent the foreseeable harms to Plaintiff and the Class which would naturally result from Payment Card Data theft.

56. Defendant negligently allowed payment card magnetic stripe information to be compromised by failing to take reasonable steps against an obvious threat.

57. In addition, in the years leading up to the Eddie Bauer Data Breach, and during the course of the breach itself and the investigation that followed, Eddie Bauer failed to follow the guidelines set forth by the FTC. Furthermore, by failing to have reasonable data security measures in place, Eddie Bauer engaged in an unfair act or practice within the meaning of §5 of the FTC Act.

58. As a result of the events detailed herein, Plaintiff and members of the Class have been and continue to be forced to protect their customers and avoid fraud losses by cancelling and reissuing cards with new account numbers and magnetic stripe information.

59. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the Class, all of which were proximately caused by Defendant's negligence. As a result of the events detailed herein, Plaintiff and members of the Class suffered losses resulting from the Eddie Bauer Data Breach related to: (a) reimbursement

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as cancelling compromised cards and purchasing and mailing new cards to their customers.

60. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

CLASS ACTION ALLEGATIONS

61. Plaintiff brings this action individually and on behalf of all other financial institutions similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure. The proposed Class is defined as:

> All Financial Institutions − including, but not limited to, banks and credit unions − in the United States (including its Territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card issuing services, whose customers made purchases from Eddie Bauer stores from January 2, 2016 to the present (the "Class").

62. Excluded from the Class are Defendant and its subsidiaries, franchises, and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

63. Plaintiff is a member of the Class it seeks to represent.

64. The Class is so numerous that joinder of all members is impracticable.

65. The members of the Class are readily ascertainable.

66. Plaintiff's claims are typical of the claims of all members of the Class.

67. The conduct of Defendant has caused injury to Plaintiff and members of the Class in substantially the same ways.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

68. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendant.

69. Plaintiff will fairly and adequately represent the interests of the Class.

70. Defendant has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

71. Plaintiff is represented by experienced counsel who are qualified to litigate this case.

72. Common questions of law and fact predominate over individualized questions. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

73. There are questions of law and fact common to all members of the Class, the answers to which will advance the resolution of the claims of the Class members and that include, without limitation:

a) whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

b) whether the conduct of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

c) whether Defendant's actions were negligent;

d) whether Defendant owed a duty to Plaintiff and the Class;

e) whether the harm to Plaintiff and the Class was foreseeable;

f) whether Defendant's actions violated RCW 19.255.020;

g) whether Defendants actions were unfair, deceptive, or both, in violation of RCW Ch. 19.86;

h) whether Plaintiff and members of the Class are entitled to injunctive relief; and

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

i) whether Plaintiff and members of the Class are entitled to damages and the measure of such damages.

COUNT ONE

NEGLIGENCE

74. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

75. Defendant owed – and continues to owe – a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and processing Plaintiff's customers' personal and financial information.

76. Defendant owed a duty to Plaintiff and the Class to provide adequate security to protect their mutual customers' personal and financial information.

77. Eddie Bauer has a common law duty to prevent the foreseeable risk of harm to others, including the Plaintiff and the Class. It was certainly foreseeable to Eddie Bauer that injury would result from a failure to use reasonable measures to protect Payment Card Data and to provide timely notice that a breach was detected. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Payment Card Data belonging to millions of Eddie Bauer customers; thieves would use Payment Card Data to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud by cancelling and reissuing the compromised cards and reimbursing their customers for fraud losses; and that the resulting financial losses would be immense.

78. Eddie Bauer assumed the duty to use reasonable security measures as a result of its conduct.

79. Eddie Bauer's duty to use reasonable data security measures also arose under §5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Payment Card Data by businesses such as Eddie Bauer. The FTC publications and

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

data security breach orders described above further form the basis of Eddie Bauer's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the part of Eddie Bauer.

80. Defendant breached its duties by: (1) allowing a third-party intrusion into their computer systems; (2) failing to protect against such an intrusion; (3) failing to maintain updated EMV card systems, updated POS terminals, and secure systems and software necessary to prevent such an intrusion; and (4) allowing the personal and financial information of customers of Plaintiff and the Class to be accessed by third parties on a large scale.

81. Defendant knew or should have known of the risk that its POS terminals could be infiltrated using methods similar or identical to those previously used against major retailers in recent months and years.

82. Defendant knew or should have known that its failure to take reasonable measures to protect its POS terminals against obvious risks would result in harm to Plaintiff and the Class.

83. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

COUNT TWO

NEGLIGENCE *PER SE*

84. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

85. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Eddie Bauer, of failing to use reasonable measures to protect Payment Card

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Data. The FTC publications and orders described above also form part of the basis of Eddie Bauer's duty.

86. Eddie Bauer violated §5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Card Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Eddie Bauer's conduct was particularly unreasonable given the nature and amount of Payment Card Data it obtained and stored and the foreseeable consequences of a data breach at an international retailer, including, specifically, the immense damages that would result to consumers and financial institutions.

87. Eddie Bauer's violation of §5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

88. Plaintiff and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses. Moreover, many of the Class members are credit unions, which are organized as cooperatives, whose members are consumers.

89. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

90. As a direct and proximate result of Eddie Bauer's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to protect themselves and their customers. They also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT THREE

DECLARATORY AND INJUNCTIVE RELIEF

91. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

92. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

93. An actual controversy has arisen in the wake of the Eddie Bauer Data Breach regarding its common law and other duties to reasonably safeguard Payment Card Data. Plaintiff alleges that Eddie Bauer's data security measures were inadequate and remain inadequate. Furthermore, Plaintiff continues to suffer injury as additional fraudulent charges are being made on payment cards issued to Eddie Bauer customers.

94. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Eddie Bauer continues to owe a legal duty to secure its customers' personal and financial information – specifically including information pertaining to credit and debit cards used by Eddie Bauer customers – and to notify financial institutions of a data breach under the common law, §5 of the FTC Act, PCI DSS standards, its commitments, and various state statutes;

(b) Eddie Bauer continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

(c) Eddie Bauer's ongoing breaches of its legal duty continue to cause Plaintiff harm.

95. The Court also should issue corresponding injunctive relief requiring Eddie Bauer to employ adequate security protocols, consistent with industry standards, to protect its Payment Card Data. Specifically, this injunction should, among other things, direct Eddie Bauer to:

(a) utilize industry standard encryption to encrypt the transmission of cardholder data at the point-of-sale and at all other times;

(b) implement encryption keys in accordance with industry standards;

(c) implement EMV technology;

(d) engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

(e) audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

(f) regularly test its systems for security vulnerabilities, consistent with industry standards;

(g) comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and

(h) install all upgrades recommended by manufacturers of security software and firewalls used by Eddie Bauer.

96. If an injunction is not issued, Plaintiff will suffer irreparable injury and lacks an adequate legal remedy in the event of another data breach at Eddie Bauer. The risk of another such breach is real, immediate, and substantial. If another breach at Eddie Bauer occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for out

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

of pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable and reputational damage.

97. The hardship to Plaintiff and the Class, if an injunction is not issued, exceeds the hardship to Eddie Bauer if an injunction is issued. Among other things, if another massive data breach occurs at Eddie Bauer, Plaintiff and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Eddie Bauer of complying with an injunction, by employing reasonable data security measures, is relatively minimal and Eddie Bauer has a pre-existing legal obligation to employ such measures.

98. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Eddie Bauer, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

COUNT FOUR

VIOLATION OF RCW 19.255.020

99. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

100. The Washington Legislature, in an effort to combat cybercrime and to protect financial institutions from negligent practices of retailers, enacted RCW 19.255.020, which states in pertinent part:

> If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

101. Plaintiff and other Class members are "financial institutions" within the meaning of RCW 19.255.020.

102. Defendant is a "business" within the meaning of RCW 19.255.020.

103. The information compromised in the Eddie Bauer Data Breach was "account information" within the meaning of RCW 19.255.020.

104. Defendant failed to take reasonable care to guard against unauthorized access of account information by, *inter alia*, failing to comply with the standards put forth by the PCI DSS, which standards Defendant must abide by in order to exercise reasonable care.

105. Such failure to take reasonable care on the part of Defendant led to Plaintiff and other Class members to incur costs associated with mitigating against fraud affecting their customers, arising from Defendant's wrongful acts.

106. Pursuant to RCW 19.255.020, Plaintiff and other Class members are entitled to reasonable actual costs related to the reissuance of credit cards and debit cards incurred to mitigate potential current or future damages to credit card and debit card holders.

COUNT FIVE

VIOLATION OF RCW Ch. 19.86.

107. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

108. Washington's Consumer Protection Act, RCW Ch. 19.86 ("CPA"), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

109. To achieve that goal, the CPA prohibits any person from using "unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce . . ." RCW 19.86.020.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

110. Eddie Bauer's policies and practices relating to its sub-standard security measures for the use and retention of its customers' financial information are unfair, deceptive, or both and violate the CPA.

111. Specifically, Eddie Bauer violated, and continues to violate, the CPA by failing to take proper precautionary measures with its payment card processing machines, evidenced, *inter alia*, by its failure to comply with the PCI DSS.

112. Similarly, Eddie Bauer violated, and continues to violate, the CPA by failing to put a fulsome notification policy in place, where customers' financial information is compromised as a result of a data breach.

113. Plaintiff and the Class seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the CPA.

114. As a result of Eddie Bauer's violations of the CPA prohibiting unfair and deceptive acts and practices, Plaintiff and members of the Class have suffered monetary damages for which Eddie Bauer is liable.

115. As redress for Eddie Bauer's repeated and ongoing violations, Plaintiff and the Class are entitled to, *inter alia*, actual damages, exemplary damages, attorney's fees, and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendant and in favor of Plaintiff and the Class and award the following relief:

A. That this action be certified as a class action, pursuant to Fed. R. Civ. P. 23, declaring Plaintiff as representative of the Class and Plaintiff's counsel as counsel for the Class;

B. Monetary damages;

C. Injunctive relief;

D. Reasonable attorneys' fees and expenses, including those related to experts and consultants;

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

E. Costs;

F. Pre- and post-judgment interest; and

G. Such other relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff, individually and on behalf of the Class, demands a trial by jury for all issues so triable.

DATED this 7th day of March, 2017.

TOUSLEY BRAIN STEPHENS PLLC

By: */s/ Kim D. Stephens*
Kim D. Stephens, WSBA #11984
kstephens@tousley.com

By: */s/ Chase C. Alvord*
Chase C. Alvord, WSBA #26080
calvord@tousley.com
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Telephone: 206.682.5600
Fax: 206.682.2992

Joseph P. Guglielmo
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com

Erin G. Comite
Stephen J. Teti
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Telephone: (860) 537-5537
Facsimile: (860) 537-4432
ecomite@scott-scott.com
steti@scott-scott.com

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Gary F. Lynch
CARLSON LYNCH SWEET KILPELA
& CARPENTER, LLP
1133 Penn Avenue, 5th floor
Pittsburg, PA 15212
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com

Karen H. Riebel
Kate Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter@locklaw.com

Arthur M. Murray
MURRAY LAW FIRM
650 Poydras St., Suite 2150
New Orleans, LA 70130
Telephone: (504) 525-8100
Facsimile: (504) 284-5249
amurray@murray-lawfirm.com

Brian C. Gudmundson
ZIMMERMAN REED, LLP
1100 IDS Center, 80 South 8th St.
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2921
bbleichner@chestnutcambronne.com

Attorneys for Plaintiff Veridian Credit Union