The Honorable James L. Robart

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. 2:17-cv-00356-JLR

SECOND AMENDED 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"). Plaintiff alleges the following based on personal knowledge, where applicable, information and belief, and the investigation of counsel:

INTRODUCTION

1. Plaintiff brings this 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] This breach compromised the names, credit and debit card numbers,

[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

card expiration dates, card verification values ("CVVs"), and other credit and debit card information (collectively, "Payment Card Data") of thousands of customers at all of Defendant's approximately 370 American and Canadian retail locations (hereinafter, the "Eddie Bauer Data Breach").

2. The Eddie Bauer Data Breach was directly caused by Defendant's failure to adequately secure its data networks and is 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, Wendy's and Kmart. Still, even with the knowledge that such data breaches were occurring throughout the retail industry and despite the warnings received from Visa, MasterCard, and American Express, Defendant failed to protect sensitive payment card information properly.

3. 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 systematically failed to maintain adequate data security measures, implement best practices, upgrade security systems, and comply with industry standards. Rather, Eddie Bauer allowed hackers to infiltrate its computer and point of sale systems and steal financial institutions' payment card and customer information. 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 hackers might have breached its computer and point of sale systems.

4. Eddie Bauer, as a Washington-based corporation, understands its dual obligation to secure and protect payment card information properly and to implement adequate data security measures to detect and prevent a data breach. Indeed, in 2010, the State of Washington enacted a regulation that mandates merchants, like Eddie Bauer, take reasonable measures to

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

protect payment card data and specifically holds merchants liable for failing to protect such information when a data breach occurs. Specifically, the Revised Code of Washington Annotated states:

> 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.

RCW 19.255.020.

5. 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. Visa implemented minimum EMV Chip Card and Terminal Requirements in October 2015. However, at the time of the Eddie Bauer Data Breach, Defendant had not fully implemented EMV technology in its stores, leaving all of the information on the magnetic stripe of cards used in its retail locations vulnerable to theft in a way about which it has repeatedly been warned.

6. Defendant exacerbated the injury by failing to notify customers of the infiltration until at least six weeks after third parties first informed Defendant the Eddie Bauer Data Breach had occurred, and after failing itself to detect the malware infecting its store payment data systems until July or even August 2016. As a result, the volume of data stolen over more than six months was much greater than it would have been had Defendant maintained sufficient malware monitoring to identify and eliminate the breach as it was occurring.

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

7. As a direct and proximate consequence of Defendant's negligence, hackers stole vast amounts of customer information 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 370 American and Canadian locations have had their credit and debit numbers compromised and their privacy rights violated, have been exposed to the risk of fraud and identity theft, and have otherwise suffered damages.

8. As a result, 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 Eddie Bauer Data Breach in one or more ways, including but not limited to: (a) notify customers of issues related to the Eddie Bauer Data Breach; (b) cancel or reissue credit and debit cards affected by the Eddie Bauer Data Breach; (c) close and/or open or reopen any deposit, transaction, checking, or other accounts affected by the Eddie Bauer Data Breach; (d) refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Eddie Bauer Data Breach; (e) respond to a higher volume of cardholder complaints, confusion, and concern; (f) increase fraud monitoring efforts; and/or (g) incur other lost revenues as a result of the breach.

9. 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.

10. Plaintiff and the members of the Class bring claims for negligence, violation of RCW 19.255.020, violation of RCW Ch. 19.86, seeking damages and declaratory and injunctive relief.

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

PARTIES

11. Plaintiff Veridian Credit Union ("Veridian" or "Plaintiff") is an Iowa-chartered credit union with its principal place of business located in Waterloo, Iowa. Veridian has thousands of checking, savings and deposit customers located in Iowa and throughout the United States, including hundreds of checking, savings, and deposit customers located in Washington State.

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

JURISDICTION AND VENUE

13. 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 it maintains its principal place of business.

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

15. Venue is proper in this Court under 28 U.S.C. §1391 because Defendant is headquartered and resides in this judicial district, its senior officers are located in this judicial

[2] See Company Info, available at http://www.eddiebauer.com/company-info/company-info-about-us.jsp (last accessed June 4, 2017).

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

district and Defendant 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 Payment Card Processing

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

17. Eddie Bauer stores accept customer payment cards for the purchase of goods and services. At the point of sale ("POS"), customers swipe these cards on a POS terminal and enter either a personal identification number (or some other confirmation number) or sign a receipt to complete the transaction.

18. 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 The Home Depot, Target, Kmart, Wendy's, P.F. Chang's, and many others. Despite widespread publicity and industry alerts regarding these other notable data breaches, Eddie Bauer failed to take reasonable steps to protect its computer systems from being breached.

19. Eddie Bauer makes a large portion of its sales to customers who use credit or debit cards. When a customer uses a credit or debit card, the transaction involves four primary parties: (1) the "merchant" (*e.g.*, Eddie Bauer) where the purchase is made; (2) an "acquiring bank" (which typically is a financial institution that contracts with the merchant to process its payment card transactions); (3) a "card network" or "payment processor" (such as Visa and MasterCard); and (4) the "issuer" (which is a financial institution – such as Plaintiffs – that issues credit and debit cards to its customers).

[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

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

- *Authorization* – when a customer presents a card to make a purchase, Eddie Bauer requests authorization of the transaction from the card's issuer;
- *Clearance* – if the issuer authorizes the transaction, Eddie Bauer completes the sale to the customer and forwards a purchase receipt to the acquiring bank with which it has contracted;
- *Settlement* – the acquiring bank pays Eddie Bauer for the purchase and forwards the receipt to the issuer, which then reimburses the acquiring bank; and
- *Post-Settlement* – the issuer posts the charge to the customer's credit or debit account.

21. Merchants acquire a substantial amount of information by processing payment card transactions, including a customer's full name; credit or debit card account number; card security code (the value printed on the card or contained on the microprocessor chip or magnetic stripe of a card and used to validate card information during the authorization process); the card's expiration date and verification value; and the PIN number for debit cards. A merchant's computer system typically stores this information and transmits it to third parties to complete the transaction. At other times, and for other reasons, merchants may also collect other personally identifiable information about their customers, including, but not limited to, financial data, mailing addresses, phone numbers, driver's license numbers, and email addresses.

22. For years, Eddie Bauer has stored in its computer systems massive amounts of customer Payment Card Data. Eddie Bauer uses this information to process payment card transactions in connection with sales to its customers and to generate profits by sharing the information with third-party affiliates, to recommend additional services to customers, and to

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

employ predictive marketing techniques. In sum, Payment Card Data is an asset of considerable value to both the Company and to hackers, who can easily sell this data on "open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[4]

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

24. 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 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.

B. The Eddie Bauer Data Breach

25. 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.

26. 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."

[4] *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016, 10:47 AM), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited July 22, 2016).

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

27. Despite notice from KrebsOnSecurity in early July 2016, Eddie Bauer did not officially confirm the Eddie Bauer Data Breach until it released a statement ***over six weeks later***, on August 18, 2016, saying that Defendant had found malware on its registers at approximately 370 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."

28. 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, 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.

29. 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.

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

31. Eddie Bauer set up 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.

32. 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

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

> 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.

33. 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."

34. 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.[5]

35. On August 25, 2016, Visa issued a Compromised Account Management System ("CAMS") alert to at least some financial institutions, indicating that the estimated fraud "exposure window" for the Eddie Bauer data breach ran from February 10, 2016 through July 15, 2016. The CAMS alert further indicated that both Track 1 and Track 2 data, which generally includes credit and debit card information, such as cardholder name, primary account number, and in certain instances, PIN number, may have been compromised in the data breach. The CAMS alert further stated that,

> Visa Fraud Control and Investigations has been notified of a confirmed network intrusion that has put Visa accounts at risk. The reported incident involves confirmed unauthorized access to a retail merchant's database of customer information that included

[5] See Open Letter to the Eddie Bauer Community from M. Egeck, CEO, available at http://cardnotification.kroll.com/ (last visited June 4, 2017).

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

> full track one and two data. Our investigators have determined, from the information available, that customer data may have been exposed on transactions covered by the exposure window noted above.

36. On September 6, 2016, Visa issued an updated CAMS alert expanding the "exposure window" for the Eddie Bauer data breach from January 4, 2016 through July 16, 2016. On November 7, 2016 Visa issued an updated CAMS alert stating that the network intrusion had been confirmed and expanded the "exposure window" for the Eddie Bauer data breach from January 1, 2016 through July 16, 2016. The November 7, 2016 CAMS alert identified that Track 1 and Track 2 data might have been exposed. On November 9, 2016, Visa issued another follow-up CAMS alert identifying that the primary account number and expiration date data elements may have also been exposed.

37. Brian Krebs, who first reported the Eddie Bauer data breach over a month before the Company admitted it, commented, "[g]iven the volume of point-of-sale malware attacks on retailers and hospitality firms in recent months, it would be nice if each one of these breach disclosures didn't look and sound exactly the same."[6]

38. Even now, almost a year 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.

39. Up to, and including, the period during which the Eddie Bauer data breach occurred, Eddie Bauer's POS and data security systems suffered from many deficiencies that made them susceptible to hackers, including, without limitation, the following:

(a) Eddie Bauer ignored well-known warnings that its POS system was susceptible to data breach;

---

[6] Credit Union Times, *Eddie Bauer Breach May Affect Six Months of Card Data,* August 31, 2017.

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

(b) Eddie Bauer failed to timely upgrade its POS software to remedy security vulnerabilities;

(c) Eddie Bauer failed to implement certain security initiatives such as tokenization and point-to-point encryption, thereby knowingly allowing data security deficiencies to persist;

(d) Eddie Bauer failed to utilize other basic security measures to protect the POS environment, such as firewalls and multi-factor login authentication to prevent hackers from accessing Payment Card Data, and software to monitor and track access to the POS Environment, which would have detected the presence of hackers and prevented Payment Card Data from being stolen;

(e) Eddie Bauer failed to upgrade its payment systems to utilize EMV technology, which would have provided better security for Payment Card Data; and

(f) Eddie Bauer operated its point-of-sale systems on an outdated operating system, which was highly vulnerable to attack because the manufacturer no longer provided security or technical updates.

C. Numerous Deficiencies in Eddie Bauer's IT and Security Systems Caused Eddie Bauer to Be Susceptible to a Data Breach

1. Despite Well-Known Risks, Eddie Bauer's Minimalistic Approach to POS Systems Security Contributed to the Data Breach

40. Much of the blame for the state of Eddie Bauer's data security systems can be placed squarely on the shoulders of the Company's management and IT support, who were incompetent and failed to maintain a system of accountability for data security. Indeed, Eddie Bauer's senior management was aware of the primary security deficiencies that left Payment Card Data at risk, yet failed to take the necessary steps to remediate such deficiencies.

41. A former Information Security Manager ("IS Manager") described Eddie Bauer management's approach toward the security of its POS environment as minimalistic and low priority. The IS Manager explained that Eddie Bauer management did not timely upgrade POS

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

security patches, and refused to implement recommended critical data security measures due to cost. The IS Manager specifically stated that Eddie Bauer had a bare minimum approach to compliance with PCI-DSS.

42. Eddie Bauer did not maintain even the most basic security measures to protect the POS systems, such as proper firewalls, multi-factor login authentication, and software to monitor and track access to the POS environment.

43. The Payment Card Industry Security Standards Council, which was founded by American Express, Discovery Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc., has issued a reference guide which describes the best security practices to comply with the Payment Card Industry's Data Security Standards ("PCI DSS"). As discussed more fully below, part of those best practices includes developing and maintaining secure systems and applications by timely and appropriately implementing security patching.

44. Had Eddie Bauer implemented proper data security measures and 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, in its 2014 annual report the *Online Trust Alliance,* a non-profit organization whose mission is to enhance online trust, user empowerment, and innovation, estimated that 740 million records were stolen in 2013 and that 89% of data breaches occurring in that year were avoidable.

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

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

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.*

46. Eddie Bauer was aware of the threat of a data breach given the prior high-profile breaches that occurred at Target, Home Depot, Wendy's and others. Indeed, Visa warned merchants, including Eddie Bauer, as early as August 2013 of malware targeting point-of-sale systems. Specifically, the alert, entitled "Retail Merchants Targeted by Memory-Parsing Malware," warned: "Since January 2013, Visa has seen an increase in network intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane."[8]

47. In February 2014, Visa again warned Eddie Bauer and other merchants of the increased risks posed by malware designed to target points-of-sale in an update to its August 2013 security alert. Specifically, the February 2014 alert stated:

> Visa is issuing this alert to make clients aware of new malware information and to remind Visa merchants to secure their payment processing (and non-payment) networks from unauthorized access. Visa highly recommends merchants implement these signatures on security solutions to detect a suspected breach. However, Visa recommends performing sufficient due diligence prior to implementing any block to avoid any inadvertent connectivity issues for legitimate access.[9]

48. In November 2015, Visa issued another security alert notifying Eddie Bauer and other merchants of additional malware infections targeting and impacting merchants' point of sale systems. This alert specifically stated this form of malware attack had targeted a restaurant

---

[8] Data Security Alert, Visa, Retail Merchants Targeted by Memory-Parsing Malware - *UPDATE* (August 2013), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf (last accessed June 4, 2017).

[9] Data Security Alert, Visa, Retail Merchants Targeted by Memory-Parsing Malware - *UPDATE* (Feb. 2014), available at https://usa.visa.com/dam/VCOM/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf (last accessed June 4, 2017).

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

group and that "infections started in August 2015 but appeared to increase dramatically in the middle of October 2015."[10] The security alert further stated that "Windows XP and Windows 7 (both 32 bit and 64 bit) are the primary operating systems infected." *Id*. However, despite these numerous warnings and alerts, Eddie Bauer failed to take reasonable steps to upgrade and protect Payment Card Data. Indeed, Eddie Bauer has known for years that a breach of its point-of-sale systems was possible and could cause serious disruption to its business and damage to payment card issuers.

49. In addition to ignoring Visa's explicit warnings, 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, to which all merchants are required to adhere as members of the payment card industry.

50. 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 compliant . . . . Obviously, based on that evidence, while a good step in the right direction, PCI is not sufficient to protect against breaches."[11]

51. 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.

---

[10] Security Alert, Visa, UPDATE - CYBER CRIMINALS TARGETING POINT OF SALE INTEGRATORS (Nov. 13, 2015), available at https://usa.visa.com/dam/VCOM/download/merchants/alert-pos-integrators.pdf (last accessed June 4, 2017).

[11] Sean Michael Kerner, *Eddie Bauer Reveals It Was the Victim of a POS Breach*, EWEEK (Aug. 19, 2016), available at http://www.eweek.com/security/eddie-bauer-reveals-it-was-the-victim-of-a-pos-breach.html (last visited June 4, 2017).

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

52. 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.

53. 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.[12]

54. 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.

55. 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.

56. 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

[12] *See* United States Computer Emergency Readiness Team, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (Aug. 27, 2014), available at https://www.us-cert.gov/ncas/alerts/TA14-212A (last visited June 4, 2017).

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

made no overtures to the card-issuing institutions that are left to pay for damages as a result of the breach.

2. Eddie Bauer Failed to Timely Patch POS Software to Fix Security Vulnerabilities and Implemented Poorly Designed Software Patches

57. The IS Manager also stated that Eddie Bauer refused to timely patch or update vital software programs to remove the "bugs" and other vulnerabilities that would render the Company's POS system/environment more susceptible to a potential data breach. The IS Manager stated that Eddie Bauer would only perform such POS-related software patching on a quarterly basis and not on a monthly basis, which in the IS Manager's opinion is a best practice.

58. Significantly, the failure to timely perform security patching on a monthly basis is a violation of PCI-DSS Requirement 6 which requires entities that process, store or transmit cardholder data and/or sensitive authentication data to "[d]evelop and maintain secure systems and applications."[13] Part of maintaining secure systems and applications includes timely upgrades to security patching. The PCI reference guide states that security patching, which involves updating software to eliminate bugs and vulnerabilities, is a best practice to prevent a potential data breach. The PCI reference guide further states that: "[s]ecurity vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. ***Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation***." *Id*. (emphasis added).

59. The PCI reference guide goes on to state that merchants should install "applicable vendor-supplied security patches. ***Install critical security patches within one***

[13] PCI DSS Quick Reference Guide: Understanding the Payment Card Industry, Data Security Standard version 3.1, available at https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf at 17 (last accessed June 4, 2017).

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

month of release." *Id*. (emphasis added). Thus, Eddie Bauer's failure to timely implement security patches exposed the Company to unnecessary risk of a data breach and violated PCI-DSS standards and best practices which require the Company to timely implement security patches.

60. According to the IS Manager and the IT Consultant, all Eddie Bauer stores throughout the United States and Canada utilized the Oracle ORPOS POS system.

61. In January 2016—the very month that Eddie Bauer admits its stores were first hacked—Oracle released a Critical Patch Update Advisory to its customer base for its POS systems (the January 2016 Oracle Update). As defined by Oracle, *A Critical Patch Update (CPU) is a collection of patches for multiple security vulnerabilities. Critical Patch Update patches are usually cumulative, but each advisory describes only the security fixes added since the previous Critical Patch Update advisory*.[14]

62. In connection with the January 2016 update, Oracle further stated in pertinent part, "***Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released fixes. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update fixes without delay***."[15] The January 2016 Oracle Update included critical patches for, among other Oracle products, the ORPOS POS system. On information and belief, Eddie Bauer did not timely implement the January 2016 Oracle ORPOS POS system updates.

[14] See Oracle Critical Patch Update Advisory – January 2016 (available at https://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html) (last accessed June 4, 2017).

[15] Id.

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

3. Eddie Bauer Failed to Implement Point-to-Point Encryption and Tokenization of the POS Environment

63. The IS Manager also described Eddie Bauer's management as unwilling to spend money on enhancements to protect the POS environment and refused to implement specific security initiatives to safeguard payment card data.

64. Specifically, the former IS Manager stated that in 2014 and 2015, Eddie Bauer retained a third party IT consulting company that performed an evaluation of Eddie Bauer's payment systems and identified two primary security initiatives: implement (a) point-to-point encryption and (b) tokenization of the POS environment.

65. An IT consultant ("IT Consultant") from the IT consulting company confirmed the IT consulting company recommended encryption and tokenization for Eddie Bauer's POS environment throughout all of its stores in the U.S. and Canada.

66. The IS Manager along with the IT consulting company strongly recommended that Eddie Bauer implement point-to-point encryption, which would encrypt Payment Card Data throughout the payment card process. The IT Consultant stated that the security initiative would have upgraded POS-related hardware, including ensuring that PIN pads were capable of encryption and installing and upgrading firmware.

67. The Payment Card Industry has published a guide on point-to-point encryption and its benefits in securing Payment Card Data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[16] Had Eddie Bauer implemented a P2PE solution prior to the data breach and a hacker were to steal encrypted Payment Card

[16] Securing Account Data with the PCI Point –to-Point Encryption Standard v2, available at https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last accessed June 4, 2017).

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

Data, that data would have been commercially worthless to the hacker as the hacker would not be able to decrypt the data to obtain the information necessary to make fraudulent purchases.

68. The IS Manager along with the IT consulting company also recommended that Eddie Bauer implement tokenization of the POS environment, which would allow Payment Card Data to be substituted with alternative data so that thieves would not be able to obtain the payment card data in transit from Eddie Bauer to the issuing and acquiring banks.

69. The Payment Card Industry defines Tokenization as "a process by which a surrogate value, called a "token," replaces the primary account number (PAN) and, optionally, other data."[17] Tokenization essentially removes the Payment Card Data from the transaction so that a potential hacker would not find, much less be able to steal, Payment Card Data because that data had been replaced by a token. Had Eddie Bauer implemented tokenization before the data breach and a hacker were to steal the tokenized information that data would have been commercially worthless to the hacker as the information would not contain any of the credit or debit card information necessary to make fraudulent purchases.

70. The IS Manager stated that cost was a primary reason why Eddie Bauer's executives did not wish to go forward with these initiatives regarding encryption and tokenization and the IT Consultant confirmed that the Company did not proceed with the initiative due to cost considerations.

4. Eddie Bauer Failed to Utilize Other Basic Security Measures, Such as Firewalls, Multi-Factor Login Authorization, and Software to Monitor and Track Access to the POS Environment

71. 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.

[17] PCI Security Standards Council Guideline: Tokenization Product Security Guidelines, available at https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf (last accessed June 4, 2017).

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

72. Eddie Bauer should have been aware of the PCI DSS requirements and the significant risks associated with a deficient or non-existent firewall and the risk that such deficiencies could lead to a data breach. Specifically, a Visa Data Security Alert, issued in February 2014, warned merchants, such as Eddie Bauer, that they should be vigilant with respect to their firewalls and firewall configuration. The February 2014 security alert informed merchants they should:

> [r]eview your firewall configuration and ensure only allowed ports, services and IP (internet protocol) addresses are communicating with your network. This is especially critical on outbound (e.g., egress) firewall rules, where compromised entities allow ports to communicate to any IP on the Internet. Hackers will leverage this misconfiguration to exfiltrate data to their IP address.[18]

73. Moreover, PCI-DSS Requirement 1, requires entities that process, store or transmit cardholder data and/or sensitive authentication data "[i]nstall and maintain a firewall configuration to protect cardholder data." Despite this, Eddie Bauer failed to take necessary measures to maintain an adequate firewall that was properly configured to prevent hackers from penetrating its computer network.

74. The IS Manager also stated that Eddie Bauer did not implement a multi-factor authentication process for its POS environment, which would have improved the security of Payment Card Data. Multi-factor authentication is a security protocol that requires more than one type of authentication to verify the identity of a user at the time of log-in for a particular application or program. Multi-factor authentication provides an additional layer of security as a hacker would not be able to access a system simply by stealing a user's log-in password. Rather, the hacker must also obtain access to that user's second level of information to access a system. PCI-DSS Requirement 8 recommends that multi-factor authentication be implemented in connection with direct and remote access to a company's systems. Specifically, PCI-DSS

[18] Data Security Alert, Visa, Retail Merchants Targeted by Memory-Parsing Malware - UPDATE (Feb. 2014), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf (last accessed June 4, 2017).

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

Requirement 8 states: "[a]ssign a unique ID to each person with computer access." Requirements 8.2 and 8.3 require that entities that process, store or transmit cardholder data and/or sensitive authentication data that they employ two-factor authentication for all users and also implement two-factor authentication for remote access to the network by its employees.[19]

75. As evidenced by the duration of the Data Breach, Eddie Bauer also failed to track access to its network adequately and to monitor the network for unusual activity, particularly on its point-of-sale terminals, which would have allowed Eddie Bauer to detect and potentially prevent hackers from stealing Payment Card Data. One software vendor, Symantec, provides the following explanation regarding its endpoint protection software: "Symantec's network threat protection technology analyzes incoming data and blocks threats while they travel through the network before hitting endpoints. Rules-based firewall and browser protection are also included to protect against web-based attacks."[20]

76. Specifically, had Eddie Bauer implemented proper endpoint detection and prevention systems, it would have been able to identify suspicious activity occurring within Eddie Bauer's network rather than allowing hackers to steal Payment Card Data for approximately eight months. Proper endpoint detection also would have triggered warnings and alerted Eddie Bauer to the transmission of Payment Card Data within its systems and alerted Eddie Bauer to large volumes of data being removed, or exfiltrated, from its network.

5. Eddie Bauer Failed to Upgrade Its Payment Systems to Utilize EMV Technology

77. 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 strips, to store Payment Card Data. Unlike magnetic-stripe cards that use

---

[19] PCI Security Standards Council Multi-Factor Authentication, available at https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf (last accessed June 4, 2017).

[20] Data Sheet, Symantec Corporation, Symantec™ Endpoint Protection 12.1.6 (2015), https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-en.pdf (last visited June 4, 2017).

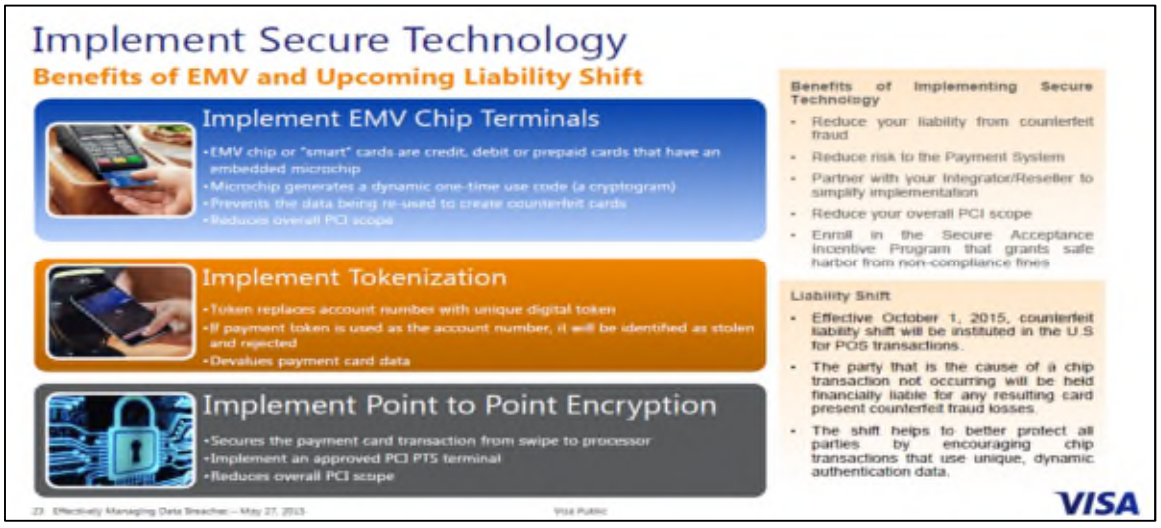
TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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 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 the stolen information.

78. 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-strip to EMV technology. Eddie Bauer did not meet that deadline.

79. 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.

80. In May 2015, Visa issued a report entitled *Effectively Managing Data Breaches*,[21] Visa presented certain best practices that large merchants should implement certain enhanced security practices, including EMV chip terminals, tokenization, and point-to-point encryption. Specifically, Visa described the benefits of these technologies to reduce a merchant's liability from counterfeit fraud:



[21] Effectively Managing Data Breaches, available at https://usa.visa.com/dam/VCOM/download/merchants/webinar-managing-data-breaches.pdf (last accessed June 4, 2017).

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

81. Indeed, as discussed above, around the same time Visa notified merchants of these technologies to prevent a data breach, the third party IT consulting company had recommended to Eddie Bauer's management that the Company implement encryption and tokenization of the POS environment. Despite Visa's and Eddie Bauer's third party IT consultant's recommendations, Defendant failed to implement these security measures that could have prevented the data breach.

D. Eddie Bauer Failed to Comply with Its Duties to Protect Payment Card Data

1. Eddie Bauer Failed to Comply with Industry Standards for Data Security

82. As the foregoing demonstrates, Eddie Bauer failed to comply with industry standards for data security.

83. 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 might 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 protect its computer systems from being breached.

84. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit Payment Card Data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of Payment Card Data, although it sets the minimum level of what must be done, not the maximum.

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

85. PCI DSS 3.1, the version of the standards in effect at the time of the data breach, impose the following 12 "high-level" mandates[22]:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	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
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

86. Among other things, PCI DSS required Eddie Bauer to secure Payment Card Data properly; not store cardholder data beyond the time necessary to authorize a transaction; to upgrade its point-of-sale software in a timely manner; to implement proper network segmentation; to encrypt Payment Card Data at the point-of-sale; to restrict access to Payment Card Data to those with a need to know; to establish a process to identify; and to fix security vulnerabilities in a timely manner. As discussed above, Eddie Bauer failed to comply with each of these requirements.

87. Furthermore, PCI DSS 3.1 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates including, *inter alia*, PCI-DSS Requirement 6 to develop and maintain secure systems and applications and PCI-DSS Requirement 8 to assign a unique ID to each person with computer access. Defendant was at all

[22] 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

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.

88. Defendant knew that because it 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.

2. Eddie Bauer Failed to Comply with Federal Trade Commission Requirements

89. 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.

90. 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 they keep; 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.

91. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security

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

plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[23]

92. 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.

E. The Data Breach Damaged Financial Institutions

93. 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.

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

95. 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.

96. 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 canceling and reissuing cards with new account numbers and magnetic stripe information.

---

[23] 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 June 4, 2017).

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

97. 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 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.

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

CLASS ACTION ALLEGATIONS

99. Plaintiff brings this action individually and on behalf of all other financial institutions similarly situated under 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 1, 2016 to the present (the "Class").

100. 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.

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

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

103. The members of the Class are readily ascertainable.

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

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

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

106. 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.

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

108. 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.

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

110. 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.

111. 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;

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

(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

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

CHOICE OF LAW

112. The application of Washington law to Eddie Bauer, as a Washington-based corporation, is appropriate because Washington has an interest in ensuring that its corporate citizens properly secure and protect payment card data and implement adequate data security measures to detect and prevent a data breach.

113. As described more fully above, Eddie Bauer's conduct, which was the cause of the data breach, was orchestrated and implemented at its corporate headquarters in Bellevue, Washington and the tortious and deceptive acts complained of occurred in, and radiated from, Washington.

114. The key wrongdoing at issue in this litigation (Eddie Bauer's failure to employ adequate data security measures) emanated from Eddie Bauer's headquarters in Washington. Indeed, Eddie Bauer's statements concerning the breach and its response thereto have come from its headquarters in Washington.

115. Eddie Bauer's executives are located in Washington, including the Chief Executive Officer and President, Chief Operating Officer and Chief Financial Officer. Moreover, the decisions that were made with respect to the protection of Payment Card Data, the data security measures, and the failure to implement adequate data security measures to prevent the Eddie Bauer Data Breach were ultimately made by the executives in Washington.

116. Washington, which seeks to protect the rights and interests of Washington and other U.S. businesses against a company doing business in Washington, has a greater interest in

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

the claims of Plaintiffs and the Class members than any other state and is most intimately concerned with the outcome of this litigation.

117. Application of Washington law to a nationwide Class with respect to Plaintiff's and the Class members' claims is neither arbitrary nor fundamentally unfair because Washington has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiffs and the nationwide Class.

118. The location where Plaintiffs were injured was fortuitous and Eddie Bauer could not have foreseen where the injury would take place, as Eddie Bauer did not know which financial institutions Eddie Bauer customers used and the location of these financial institutions' headquarters, or principal places of business, at the time of the breach.

COUNT ONE

NEGLIGENCE

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

120. Eddie Bauer owed—and continues to owe—a duty to Plaintiff and the Class to use reasonable care in safeguarding Payment Card Data and notifying them of any breach promptly, so that compromised financial accounts and credit cards can be closed quickly to avoid fraudulent transactions. This duty arises from several sources, including, but not limited to, the sources described below and is independent of any duty Eddie Bauer owed as a result of its contractual obligations.

121. Eddie Bauer has a common law duty to prevent the foreseeable risk of harm to others, including Plaintiff and the Class. Plaintiff has hundreds of checking, savings and deposit customers located in Washington State. 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

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

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.

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

123. Finally, Eddie Bauer's duty to use reasonable care in protecting Payment Card Data arose not only as a result of the common law and the statutes described herein, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

124. Eddie Bauer breached its common law, statutory, and other duties and thus was negligent by failing to use reasonable measures to protect Plaintiff's Payment Card Data from the hackers who perpetrated the data breach and by failing to provide timely notice of the breach. Upon information and belief, the specific negligent acts and omissions committed by Eddie Bauer include, but are not limited to, some, or all, of the following:

(a) failure to delete cardholder information after the time period necessary to authorize the transaction;

(b) failure to employ systems to protect against malware;

(c) failure to comply with industry standards for software and point-of-sale security;

(d) failure to regularly update its antivirus software;

(e) failure to maintain an adequate firewall;

(f) failure to track and monitor access to its network and cardholder data;

(g) failure to limit access to those with a valid purpose;

(h) failure to encrypt Payment Card Data at the point-of-sale;

(i) failure to transition to the use of EMV technology;

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

(j) failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

(k) failure to assign a unique ID to each individual with access to its systems;

(l) failure to automate the assessment of technical controls and security configuration standards;

(m) failure to adequately staff and fund its data security operation;

(n) failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

(o) failure to recognize red flags signaling that Eddie Bauer systems were inadequate and that, as a result, the potential for a massive data breach was increasingly likely;

(p) failure to recognize that hackers were stealing Payment Card Data from its network while the data breach was taking place; and

(q) failure to disclose the data breach promptly.

125. In connection with the conduct described above, Eddie Bauer acted wantonly, recklessly, and with complete disregard for the consequences.

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

COUNT TWO

VIOLATION OF RCW 19.255.020

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

128. The Washington Legislature, 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

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

> 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.

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

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

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

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

133. 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.

134. Under 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 THREE

VIOLATION OF RCW Ch. 19.86.

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

136. 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.

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

137. 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.

138. As alleged herein, Eddie Bauer's policies and practices relating to its sub-standard security measures for the use and retention of its customers' financial information violate the CPA because they are both unfair and deceptive.

139. Eddie Bauer had statutory, regulatory, and common law obligations to prevent the foreseeable risk of harm to others, including the Plaintiff and the Class. It was foreseeable that the failure to use reasonable measures to protect Payment Card Data and to provide timely notice that a breach was detected if reasonable security measures were not taken, put consumers, Plaintiff, and members of the Class at a serious risk of injury from the theft and fraudulent use of consumers' Payment Card Data. Moreover, it was foreseeable that as a result of the theft and fraudulent use of Payment Card Data financial institutions would be required to mitigate the fraud by canceling and reissuing the compromised cards, reimbursing their customers for fraud losses, and that the resulting financial losses would be immense.

140. Specifically, Eddie Bauer engaged in unfair acts and practices in violation of the CPA by failing to implement and maintain reasonable security measures to protect Payment Card Data, including failing to take proper precautionary measures with its payment card processing machines, failing to implement EVC chip readers, failing to comply with industry standards, and failing to comply with the PCI DSS.

141. Eddie Bauer's failure to implement and maintain reasonable security measures to protect consumers' financial information and failure to comply with industry standards and the PCI DSS were likely to, and did, cause substantial injury to consumers, Plaintiff and members of the Class. Eddie Bauer's acts or practice of maintaining inadequate security measures and failure to comply with industry standards and PCI DSS provided no countervailing benefit to consumers or competition.

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

142. As Eddie Bauer was solely responsible for securing its customer data, there is and was no way for Plaintiff and members of the Class to know about Eddie Bauer's inadequate security practices or to avoid their injuries.

143. Further, Eddie Bauer's failure to inform Plaintiff and the Class of its inadequate security practices and failure to comply with PCI DSS and industry standards, constitute deceptive acts and practices in violation of the CPA. By facilitating purchases in Eddie Bauer stores, Plaintiff and Class members reasonably believed that Eddie Bauer would follow the required PCI DSS and industry standards and implement reasonable practices and policies for the use, retention, and security of its customers' financial information to protect against the foreseeable threat of data theft and resulting harm. In light of the foreseeable risk of harm to consumers, Plaintiff and members of the Class, reasonably believed Eddie Bauer would use reasonable practices to protect Payment Card Data and comply with industry standards and PCI DSS. Eddie Bauer's acts, omissions, or practices were likely to mislead Plaintiff and members of the Class.

144. Similarly, Eddie Bauer violated and continues to violate, the CPA by failing to put a reasonable notification policy in place, where customers' financial information is compromised as a result of a data breach. The failure to notify consumers of the data breach was likely to cause additional harm to consumers, Plaintiff, and members of the Class as it allowed the theft of additional data to continue unabated, and thereby exacerbated the injuries suffered by Plaintiff and members of the Class. Eddie Bauer's duty to notify consumers, Plaintiff, and other members of the Class in a reasonable manner is not outweighed by any countervailing benefits to consumers or competition.

145. Eddie Bauer's unfair acts or practices occurred in its trade or business and have injured a substantial portion of the public. Eddie Bauer's acts, practices, or omissions are injurious to the public interest as they caused injury to, and had and have the capacity to cause

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

injury to, Plaintiff and other financial institutions, and have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of its misconduct may last for years.

146. As a direct and proximate 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.

147. 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.

148. 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 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, under 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. Declaratory and Injunctive relief;

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

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.

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

DATED this 27th day of November, 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, *pro hac vice*
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, *pro hac vice*
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

Gary F. Lynch, *pro hac vice*
Kevin W. Tucker, *pro hac vice*
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, *pro hac vice*
Kate Baxter-Kauf, *pro hac vice*
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

Kevin W. Tucker, *pro hac vice*
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
113 Penn Avenue, 5th Floor
Pittsburgh, PA 1522
Telephone: (412) 322-9243
ktucker@carlsonlynch.com

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on November 27, 2017, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered on the CM/ECF system. All other parties (if any) shall be served in accordance with the Federal Rules of Civil Procedure.

DATED at Seattle, Washington, this 27th day of November, 2017.

/s/ Chase C. Alvord
Chase A. Alvord WSBA #11984
TOUSLEY BRAIN STEPHENS PLLC

6308/001/487922.1

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