IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

BRIAN H. BLAKE and CATHERINE HARRISON individually and on behalf of all others similarly situated, Plaintiffs, v. GLOBAL PAYMENTS INC., a Georgia corporation and ACTIVE NETWORK, LLC, a Delaware limited liability company, Defendants.	)	CASE NO. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Brian H. Blake and Catherine Harrison ("Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Defendants Global Payments Inc. and ACTIVE Network, LLC ("Defendants") based on personal knowledge as to their own experiences, on information and belief, and on investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated whose personal and non-public information, including names,

credit card and debit card numbers, expiration dates, security codes (the three or four-digit value included on the front or back of payment cards and used for verification of certain transactions), and Blue Bear account usernames and passwords, (collectively, "Personal Information") was compromised in a massive security breach of Defendants' Blue Bear software platform and payment card environment between October 1, 2019 and November 13, 2019 (the "Data Breach").

2. Defendants' Blue Bear software platform and payment card environment, which includes school accounting software, a student management system, and an online school store, is used by thousands of schools and districts across the United States.

3. As a result of the Data Breach, thousands of consumers who made payments via school websites across the United States using Defendants' Blue Bear software platform and payment card environment have had their sensitive Personal Information stolen and exposed to fraudsters.

4. On or about December 30, 2019, nearly three months after the Data Breach began, Defendants announced the Data Breach to the public. At this time ACTIVE began mailing to victims of the Data Breach and filing with various State

Attorneys General a Notice of Data Breach ("Notice")[1]. Apparently, Defendants believed it was in their best interest not to immediately disclose the Data Breach to victims via email or website notices. This delay hindered Data Breach victims from taking measures to protect against fraud and identity theft.

5. Unfortunately, the Notice sent to Data Breach victims and filed with various State Attorneys General contained very little detail about the Data Breach. This lack of detail made it more difficult for victims of the Data Breach to adequately respond to the Data Breach and protect themselves from fraud and identity theft. Furthermore, as of the date of the filing of this action, Defendants have not provided victims with any post-breach reports or findings that might aid them in dealing with the aftermath of the Data Breach.

6. The Notice ACTIVE sent to Data Breach victims stated that "[a]s soon as we identified the suspicious activity, our counsel engaged a leading cybersecurity firm to investigate the incident and took steps to enhance its monitoring tools and security controls."[2] One may deduce that the referenced enhancements to

[1] Sample Notice of Data Breach filed with the Attorney General of California: https://oag.ca.gov/system/files/Individual%20Letter%20CA.pdf (last visited April 10, 2020).
[2] ACTIVE, Notice of Data Breach, supra note 1.

Defendants' monitoring tools and security controls were enhancements that could have and likely should have been in place before the Data Breach.

7. As alleged herein, Defendants' failure to implement adequate data security measures to protect their customers' sensitive Personal Information directly and proximately caused injuries to Plaintiffs and Class Members.

8. The Data Breach was the inevitable result of Defendants' inadequate data security measures and careless approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and even though these types of data breaches were and are occurring frequently throughout a myriad of industries, Defendants failed to ensure that they maintained adequate data security measures to protect customer Personal Information from criminals.

9. As a direct and proximate result of Defendants' conduct and data security negligence, a massive amount of Plaintiffs' and Class Members' Personal Information was exfiltrated from Defendants' Blue Bear software platform and payment card environment and exposed to those who would misuse that Personal Information. Victims of the Data Breach have had their sensitive Personal Information compromised, had their privacy rights violated, been exposed to the

increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise have been injured.

10. Moreover, Plaintiffs and Class Members have been forced to spend significant time associated with, among other things, closing out and opening new credit or debit card accounts, ordering replacement cards, obtaining fraud monitoring services, losing access to cash flow and credit lines, monitoring credit reports and accounts, purchasing identity theft insurance, and/or other losses resulting from the unauthorized use of their cards or accounts.

11. Rather than providing meaningful assistance to Data Breach victims to help deal with the fraud that has and will continue to result from the Data Breach, Defendants simply provided access to one year of credit monitoring and instructed Data Breach victims to "be diligent in watching for unauthorized activity[.]"[3] Credit monitoring is the bare minimum remedy that Defendants could have offered Data Breach victims and is much less than what has been frequently made available to victims of other data breaches.

12. Plaintiffs and Class Members seek to recover damages caused by Defendants' negligence, negligence *per se*, breach of implied contract, breach of contract (as third-party beneficiaries), violations of Georgia's consumer protection

[3] ACTIVE, Notice of Data Breach, supra note 1.

and data breach notification statutes, violations of Utah's consumer protection statutes, violations of Nevada's consumer protection statutes, and unjust enrichment.

PARTIES

Plaintiff Brian H. Blake

13. Plaintiff Brian H. Blake is an adult residing in Salt Lake City, Utah. During the period of time the Data Breach occurred, between October 1, 2019 and November 13, 2019, Plaintiff Blake used his credit card to pay a school fee for his child via Defendants' Blue Bear software platform and payment card environment.

14. In late-November of 2019, Plaintiff Blake received a communication from his credit card company notifying him that the credit card he used on Defendants' Blue Bear software platform and payment card environment during the Data Breach period had likely been compromised and that suspected fraudulent charges had been made. The suspected fraudulent charges were confirmed by Plaintiff Blake to be fraudulent and the card was cancelled. A new card was then issued to Plaintiff Blake by his credit card company. Prior to this, Plaintiff Blake had not experienced any fraud on this credit card.

15. As a result of this incident, Plaintiff Blake went without access to his card until his new card was delivered. Plaintiff Blake also had auto-payments connected to his card disrupted as a result of the card cancellation.

16. As a result of being victimized by the Data Breach, Plaintiff Blake was required to spend a significant amount of time addressing fraud concerns related to his compromised card and otherwise dealing with the aftermath of the Data Breach.

17. Plaintiff Blake experienced actual fraud because of the breach. Had Plaintiff Blake known Defendants would not adequately protect his Personal Information and other sensitive information entrusted to them, he would not have made payments via Defendants' Blue Bear software platform and payment card environment.

18. On or about January 2, 2020, Plaintiff Blake received ACTIVE's *Notice of Data Breach* in the mail.

19. As a result of Defendants' failure to adequately safeguard Plaintiff Blake's Personal Information, he has been injured.

Plaintiff Catherine Harrison

20. Plaintiff Catherine Harrison is an adult residing in Las Vegas, Nevada. During the period of time the Data Breach occurred, between October 1, 2019 and November 13, 2019, Plaintiff Harrison used her credit card to pay a test fee for her child via Defendants' Blue Bear software platform and payment card environment.

21. As a result of being victimized by the Data Breach, Plaintiff Harrison was required to spend a significant amount of time addressing fraud concerns and otherwise dealing with the aftermath of the Data Breach.

22. Had Plaintiff Harrison known Defendants would not adequately protect her Personal Information and other sensitive information entrusted to them, she would not have made payments via Defendants' Blue Bear software platform and payment card environment.

23. On or about January 2, 2020, Plaintiff Harrison received ACTIVE's *Notice of Data Breach* in the mail.

24. As a result of Defendants' failure to adequately safeguard Plaintiff Harrison's Personal Information, she has been injured.

Defendant Global Payments Inc.

25. Defendant Global Payments Inc. is a Georgia corporation that maintains its headquarters in Atlanta, Georgia.

26. Defendant Global Payments Inc. owns Defendant ACTIVE Network, LLC.

Defendant ACTIVE Network, LLC

27. Defendant ACTIVE Network, LLC is a Delaware limited liability company that maintains its headquarters in Dallas, Texas.

JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendants. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. § 1367.

29. This Court has personal jurisdiction over Global Payments Inc. Global Payments Inc. is Georgia corporation headquartered in Atlanta, Georgia.

30. This Court has personal jurisdiction over ACTIVE Network, LLC. ACTIVE Network, LLC has sufficient minimum contacts with the state of Georgia, including clients and consumers utilizing the Blue Bear software platform and payment card environment within this district. ACTIVE Network, LLC intentionally avails itself of clients, consumers and markets within the state of Georgia through the promotion, marketing, and sale of its products and services.

31. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because, as noted above, Global Payments Inc. is headquartered in this district and ACTIVE Network, LLC conducts substantial business in this district. A substantial

part of the events and/or omissions giving rise to the claims occurred, in part, within this district.

FACTUAL ALLEGATIONS

Defendants' Business Activities

32. Global Payments is a worldwide provider of payment technology and software solutions.

33. According to Global Payments' corporate website, it "provide[s] cutting-edge payments and software solutions all under one roof to help startups to enterprise businesses simplify commerce".[4]

34. Global Payments purportedly provides "a broad range of solutions that allow [its] customers to accept various payment types and operate their businesses more efficiently".[5]

35. On September 1, 2017, Global Payments added ACTIVE Network to its stable of companies for total purchase consideration of $1.2 billion.

36. According to ACTIVE, it "offers intelligent and intuitive registration, secure payment processing, insightful data and services to help organizers drive

[4] https://www.globalpaymentsinc.com/en-us/about-us (last visited April 10, 2020).
[5] https://www.globalpaymentsinc.com/en-es/company (last visited April 10, 2020).

increased participation and revenue while streamlining administration."[6]

37. ACTIVE claims it "engages over 15M participants on behalf of over 27,000 organizers through [its] global marketplace for activities and events."[7]

38. According to ACTIVE's Blue Bear website, Blue Bear is the "[t]echnology partner to thousands of schools & districts".[8]

39. Defendants' Blue Bear software platform and payment card environment is a school administration software suite that provides a library of products, including school accounting software, school management software and online store software.

The Data Breach

40. On or about December 30, 2019, ACTIVE confirmed in a "Notice of Data Breach" filed with various State Attorneys General and mailed to Data Breach victims that it recently became aware of a security incident involving the Blue Bear software platform and payment card environment that compromised customers' sensitive Personal Information. The Notice provided the following:

> We are writing to inform you that we recently became aware of a security incident involving Blue Bear Software, a software platform that facilitates administration and management of school accounting,

[6]https://www.activenetwork.com/Assets/ActiveNetwork/Docs/ACTIVENetwork_CorporateFactSheet-2019.pdf (last visited April 10, 2020).
[7] https://www.activenetwork.com/home (last visited April 10, 2020).
[8] http://www.bluebearsoft.com (last visited April 10, 2020).

student fees, and online stores on behalf of educational institutions. You may have conducted business on the Blue Bear platform when you purchased items from the webstore of an educational institution. The Blue Bear platform is operated by ACTIVE Network, LLC, however, this incident did not impact other systems of ACTIVE or its affiliates.

What Happened?
We recently identified suspicious activity on the Blue Bear platform. Our investigation determined the activity related to Blue Bear webstore users between October 1, 2019 and November 13, 2019. During this time, some personal information that you provided may have been accessed or acquired by unauthorized third parties.

What Information Was involved?
While we are unable to determine with certainty whether your personal information was affected, the personal information involved may have included: name, credit card or debit card number ending in [xxxx], expiration date and security code (the three or four-digit value included on the front or back of payment cards and used for verification of certain transactions), and Blue Bear account usernames and passwords. This incident did not involve unauthorized access to Social Security numbers, driver license numbers, or similar government ID card numbers.

What We Are Doing?
We take this matter very seriously. As soon as we identified the suspicious activity, our counsel engaged a leading cybersecurity firm to investigate the incident and took steps to enhance its monitoring tools and security controls. We are also offering you free identity monitoring services. More information on how to access these services can be found below and in the enclosed reference guide.

What You Can Do
We encourage you to be diligent in watching for unauthorized activity associated with your payment card accounts and to quickly report suspicious activity to your bank or credit card company. The phone number to call is usually on the back of the credit or debit card. The Reference Guide contains additional information on steps you can take

> to monitor and protect your personal information. We have also arranged for Kroll to provide you one year of identity monitoring services at no cost to you. For instructions on how to access these complimentary services, please call the toll-free number, 1-844-967-1237. The Reference Guide contains additional information about these services.
> Your Kroll Membership Number is: []
>
> Other Important Information
> The enclosed Reference Guide also includes additional information on general steps you can take to monitor and protect your personal information.
>
> For more information
> We apologize for any inconvenience this incident may cause. You may contact us at 1-844-967-1237, Monday through Friday between 8:00 a.m. and 5:30 p.m. Central Time if you have questions or would like additional information about this incident.

41. The Notice makes clear that at Defendants' Blue Bear software platform and payment card environment did not utilize all monitoring tools, security controls and other technology available to it. Only after the breach did ACTIVE take "steps to enhance its monitoring tools and security controls."

42. It is unclear from the Notice why Defendants decided to not enhance the monitoring tools and security controls until after the Data Breach.

43. As is typical with payment card data breaches, the Data Breach was a result of malware that criminals routinely use in payment card breaches. According to CISCOMAG,

> Security pros at Active Network opined that the incident appears to be a web skimming attack, where attackers planted malicious code in Active Network's Blue Bear platform and collected users' payment details while they were paying fees.[9]

44. Furthermore, the Notice issued by ACTIVE give no indication as to the *actual* magnitude of the Data Breach, including the actual number of customers and cards affected.

45. The unfortunate reality is that Defendants have provided very limited information surrounding the Data Breach that would allow victims to protect themselves against payment card fraud and identity theft.

Industry Standards and the Protection of Customer Personal Information

46. It is well known in the retail industry that sensitive Personal Information is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in payment systems either online or in stores."[10]

---

[9] Attackers Compromised School Management Platform Blue Bear, CISCOMAG (January 6, 2020), https://www.cisomag.com/attackers-compromised-school-management-platform-blue-bear/ (last visited April 10, 2020).

[10] Dennis Green, Mary Hanbury and Áine Cain, "If you bought anything from these 19 companies recently, your data may have been stolen," BUSINESS INSIDER (November 19, 2019), available at https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited April 10, 2020).

47. Despite the known risk of POS malware intrusions and web skimming (Magecart) attacks, and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendants failed to take reasonable steps to adequately protect the Blue Bear software platform and payment card environment from being breached, and then failed to detect the Data Breach for approximately 6 weeks.

48. Defendants are, and at all relevant times have been, aware that the Personal Information they maintain as a result of purchases made via the Blue Bear software platform and payment card environment is highly sensitive and could be used for nefarious purposes by third parties. Indeed, ACTIVE acknowledged in the Notice that it took steps to enhance its monitoring tools and security controls as a result of the Data Breach.

49. Defendants' decision to utilize at least some monitoring tools and security controls in conjunction with the Blue Bear software platform and payment card environment, coupled with ACTIVE's explicit statements in its Privacy Policy, makes clear that Defendants recognized the importance of adequately safeguarding their customers' sensitive Personal Information yet failed to take the steps necessary to protect that sensitive data.

50. On its website, ACTIVE's Privacy Policy[11] that was posted during the Data Breach provided the following in part:

> **Your Privacy Rights**
>
> **Effective date:** Effective date: May 25, 2018
>
> Active Network, LLC ("ACTIVE," "us", "we" or "our") values your privacy, and we are committed to protecting your personal information.
>
> ***
>
> **Security**
>
> We have implemented and maintain appropriate technical and organisational security measures, policies and procedures designed to reduce the risk of accidental destruction, or loss, or unauthorised disclosure or access to such information appropriate to the nature of the information concerned, including:
> • (where appropriate) password protection, encryption, and use of secure communication transmission software (known as "secure socket layering" or "SSL") to protect our Sites;
> • placing confidentiality requirements on our employees and service providers;
> • destroying or permanently anonymising personal information if it is no longer needed for the purposes for which it was collected; and
> • following strict security procedures in the storage and disclosure of your personal information to prevent unauthorised access to it. Whilst we take appropriate

[11] ACTIVE, Privacy Policy, available at https://web.archive.org/web/20191029225057/www.activenetwork.com/information/privacy-policy (last visited April 10, 2020).

> technical and organisational measures to safeguard your personal information, no transmission over the Internet can ever be guaranteed to be secure. Therefore, we cannot guarantee the security of any personal information that you transfer over the Internet to us and any such transmission is at your own risk.

51. On its website, ACTIVE's current Privacy Policy[12] provides the following in part:

> **Your Privacy Rights**
>
> **Last Updated:** December 19, 2019
>
> Active Network, LLC ("ACTIVE," "us", "we" or "our") values your privacy, and we are committed to protecting your personal information.
>
> ***
>
> **Security**
>
> We have implemented and maintain appropriate technical and organisational security measures, policies and procedures designed to reduce the risk of accidental destruction, or loss, or unauthorised disclosure or access to such information appropriate to the nature of the information concerned, including:
> • (where appropriate) password protection, encryption, and use of secure communication transmission software (known as "transport layer security" or "TLS") to protect our Sites;

[12] ACTIVE, Privacy Policy, available at https://www.activenetwork.com/information/privacy-policy (last visited April 10, 2020).

> • placing confidentiality requirements on our employees and service providers;
> • destroying or permanently anonymising personal information if it is no longer needed for the purposes for which it was collected; and
> • following strict security procedures in the storage and disclosure of your personal information to prevent unauthorised access to it. Whilst we take appropriate technical and organisational measures to safeguard your personal information, no transmission over the Internet can ever be guaranteed to be secure. Therefore, we cannot guarantee the security of any personal information that you transfer over the Internet to us and any such transmission is at your own risk.

52. Furthermore, ACTIVE's Blue Bear software website[13] claims that its "intelligent online school store solution" is a "much more secure" way to collect payments. ACTIVE also states that the Blue Bear software features "secure online payments with PCI (Payment Card Industry) compliance." Benefits of the Blue Bear software purportedly also include "reduced risk of fraud" and "increased security."

53. Defendants are thus aware of the importance of safeguarding their customers' Personal Information from the foreseeable consequences that would occur if their data security systems and computer servers were breached.

[13] http://www.bluebearsoft.com/online-school-store-software.htm (last visited April 10, 2020).

54. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

55. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve 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 Global Payments and ACTIVE 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.

56. The twelve requirements of the PCI DSS are: (1) Install and maintain a firewall configuration to protect cardholder data; (2) Do not use vendor-supplied defaults for system passwords and other security parameters; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (7) Restrict access to cardholder data by business need to know; (8) Identify and authenticate access to system components; (9) Restrict physical access to cardholder

data; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel.[14]

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

58. Defendants were, at all material times, fully aware of their data protection obligations considering their participation in the payment card processing networks and their daily collection and transmission of thousands of sets of Personal Information.

59. Because Defendants accepted payment cards containing sensitive financial information, they knew that their customers were entitled to and did in fact rely on them to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

60. 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

[14] PCI SECURITY STANDARDS COUNCIL, PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1, at 9 (May 2018), available at https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1586531966831 (last visited April 10, 2020).

practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015); *see also See Consumer Data Protection: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 2358081, at *6 (June 15, 2011) (statement of Edith Ramirez, Comm'r, FTC) ("[T]he Commission enforces the FTC Act's proscription against unfair . . . acts . . . in cases where a business['s] . . . failure to employ reasonable security measures causes or is likely to cause substantial consumer injury."); *Data Theft Issues: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 1971214, at *7 (May 4, 2011) (statement of David C. Vladeck, Director, FTC Bureau of Consumer Protection) (same).

61. 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.

62. 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 such risks.[15]

63. 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 with regards to their data security obligations.

Defendants Disregarded Industry Standards for Customer Data Security

64. As noted above, Defendants should have been and, based upon their acknowledged use of at least some monitoring tools and security controls in conjunction with the Blue Bear software platform and payment card environment, were aware of the need to have adequate data security systems in place.

65. Despite this, Defendants failed to upgrade or maintain the data security systems in a meaningful way in order prevent data breaches. Defendants' security

[15] FEDERAL TRADE COMMISSION, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 10, 2020).

flaws run afoul of industry best practices and standards. More specifically, the security practices Defendants had in place with respect to the Blue Bear software platform and payment card environment are in contrast and conflict with the PCI DSS core security standards.

66. Had Defendants maintained the Blue Bear software platform and payment card environment, adequately protected them, and had adequate security safeguards in place, the Data Breach could have been prevented.

67. As a result of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented data breaches, Defendants were alerted to the risk associated with failing to ensure that the Blue Bear software platform and payment card environment were adequately secured.

68. Defendants were not only aware of the threat of data breaches, generally, but were aware of the specific danger of malware infiltration. Malware has been used recently to infiltrate large retailers such as, *inter alia*, Home Depot, Target, GameStop, Chipotle, Jason's Deli, Whole Foods, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Defendants were aware that malware is a real threat and is a primary tool of infiltration used by hackers seeking to carry out payment card breaches.

69. In addition to the publicly announced data breaches described above (among many others), Defendants knew or should have known of 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 malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[16]

70. Despite the fact that Defendants were on notice of the very real possibility of consumer data theft associated with their security practices and that Defendants knew or should have known about the elementary infirmities associated with the Blue Bear software platform and payment card environment, they still failed to make necessary changes to their security practices and protocols, and permitted massive malware intrusions to occur for approximately 6 weeks.

71. Defendants, at all times relevant to this action, had a duty to Plaintiffs and Class Members to: (a) properly secure Personal Information submitted or collected via the Blue Bear software platform and payment card environment; (b) encrypt Personal Information using industry standard methods; (c) use available

[16] See U.S. COMPUTER EMERGENCY READINESS TEAM, Alert (TA14-212A): Backoff Point-of-Sale Malware (July 31, 2014) (revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A (last visited April 10, 2020).

technology to defend their systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiffs and Class Members, which would naturally result from Personal Information theft; and (e) promptly notify victims when Defendants became aware of the likelihood that Personal Information may have been compromised.

72. Defendants permitted customers' Personal Information to be compromised by failing to take reasonable steps against an obvious threat.

73. In addition, leading up to the Data Breach, during the breach itself, and during the investigation that followed, Defendants failed to follow the guidelines set forth by the FTC.

74. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[17]

75. The Data Breach is particularly egregious and the data security failures are particularly alarming given that the Data Breach was permitted to occur for over 6 weeks. Clearly, had Defendants utilized adequate data security and data breach

[17] Lisa Baertlein, Chipotle Says Hackers Hit Most Restaurants in Data Breach, REUTERS (May 26, 2017), https://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited April 10, 2020).

precautions, the window of the Data Breach would have been significantly mitigated, and the level of impact could have been reduced, had the breach been permitted to happen at all in the first place.

76. Because payment card data breaches involving malware are so common, and given the high level of data security measures available to companies that take customer payment information in, like Defendants, there is no reason why Defendants could not have adequately protected the Blue Bear software platform and payment card environment from the Data Breach.

77. As a result of the events detailed herein, Plaintiffs and Class Members suffered actual, palpable fraud and losses resulting from the Data Breach, including: financial losses related to the purchases made via Defendants' Blue Bear software platform and payment card environment that Plaintiffs and Class Members would not have made had they known of Defendants' careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; increased risk of future

fraud and identity theft; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Personal Information.

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

79. Furthermore, the Personal Information stolen due to Defendants' actions can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.

80. To date, and as made clear in the Notice, Defendants are not taking any real measures to assist affected customers. In the first place, Defendants have released very little information about the Data Breach, leaving victims of the breach in the dark and vulnerable to continued fraud. Defendants merely provided one year of credit monitoring and instructed Data Breach victims to "be diligent in watching for unauthorized activity[.]"[18]

81. Defendants' advice makes it clear that they are shifting the responsibility for the Data Breach to victims, rather than taking real steps to assist their customers in protecting against the fraud to which Defendants exposed them. Upon information and belief, to date, Defendants are not offering identity theft insurance to customers impacted by the Data Breach.

[18] ACTIVE, Notice of Data Breach, *supra* note 1.

82. Defendants' failure to adequately protect their customers' Personal Information has resulted in consumers having to undertake various errands (e.g., obtaining identity theft insurance, checking credit reports, etc.) that require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of their own money. At the same time, Defendants are doing very little to assist those affected by the Data Breach and have withheld important details about the Data Breach as the investigation is conducted. Instead, Defendants are putting the burden on the consumer to discover possible fraudulent transactions.

CLASS ALLEGATIONS

83. Plaintiffs bring this action individually and on behalf of the following classes and subclasses (collectively "Class" or "Classes") pursuant to Fed. R. Civ. P. 23:

National Class

All persons in the United States who had their personal information compromised as a result of the Data Breach.

84. In the alternative to the National Class, Plaintiffs bring this action individually and on behalf of the following state subclasses:

Utah Class

All persons in Utah who had their personal information compromised as a result of the Data Breach.

Nevada Class

All persons in Nevada who had their personal information compromised as a result of the Data Breach.

85. Excluded from the Classes are Defendants, their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change, or expand the definitions of the Classes based on discovery and further investigation.

86. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Classes are so numerous that their individual joinder is impracticable, as the proposed Classes appear to include tens of thousands of members who are geographically dispersed. Upon information and belief, the Data Breach affected at least tens of thousands of consumers across the United States.

87. **Typicality**: Plaintiffs' claims are typical of Class Members' claims. Plaintiffs and all Class Members were injured through Defendants' uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class Member because Plaintiffs and each Class Member had their sensitive data and Personal Information compromised in the same way by the same conduct by Defendants.

88. **Adequacy**: Plaintiffs are adequate representatives of the Classes because Plaintiffs' interests do not conflict with the interests of the Classes that they seek to represent; Plaintiffs have retained counsel that are competent and highly experienced in class action litigation, including data breach cases in particular; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Classes will be fairly and adequately protected by Plaintiffs and their counsel.

89. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class Members. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits

of single adjudication, economy of scale, and comprehensive supervision by a single court.

90. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to Plaintiffs and all Class Members. These questions predominate over the questions affecting individual Class Members. These common legal and factual questions include, but are not limited to, the following:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants owed duties to Plaintiffs and Class Members to protect their Personal Information and to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class, and whether it breached these duties;
- whether Defendants violated federal and state laws as a result of the Data Breach;
- whether Defendants knew or should have known that the Blue Bear software platform and payment card environment was vulnerable to attacks from hackers and cyber-criminals;
- whether Defendants' conduct was the proximate cause of the breach of the Blue Bear software platform and payment card environment resulting

in the theft of customers' Personal Information;

- whether Defendants wrongfully failed to inform Plaintiffs and Class Members that they did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard consumers' sensitive Personal Information;
- whether Defendants failed to inform Plaintiffs and the Class Members of the Data Breach in a timely and accurate manner;
- whether Defendants have taken adequate preventive and precautionary measures to ensure the Plaintiffs and Class Members will not experience further harm;
- whether Plaintiffs and Class Members suffered injury as a proximate result of Defendants' conduct or failure to act; and
- whether Plaintiffs and Class Members are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and Class Members.

91. Defendants have acted or refused to act on grounds generally applicable to Plaintiffs and the other Class Members, thereby making appropriate final injunctive relief and declaratory relief with respect to the Classes as a whole.

92. Given that Defendants have engaged in a common course of conduct as

to Plaintiffs and the Class Members, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

93. The Classes are defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Personal Information to cyber criminals due to Defendants' failure to protect this information, adequately warn the Classes that adequate data security measures were not in place, and failure to adequately warn of the Data Breach. Class membership will be readily ascertainable from Defendants' business records, and/or from records of third parties.

94. Plaintiffs reserve the right to revise the above Class definitions and any of the averments of fact herein based on facts adduced in discovery.

COUNT I
NEGLIGENCE

95. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

96. Defendants collected Personal Information from Plaintiffs and Class Members via the Blue Bear software platform and payment card environment.

97. Defendants owed a duty to Plaintiffs and the Class Members to maintain confidentiality and to exercise reasonable care in safeguarding and

protecting their Personal Information in Defendants' possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Defendants' Blue Bear software platform and payment card environment, networks and data security systems to ensure that Plaintiffs' and Class Members' Personal Information in Defendants' possession was adequately protected in the process of collection and following collection while stored on Defendants' systems.

98. Defendants further owed a duty to Plaintiffs and Class Members to implement processes that would detect a breach of the Blue Bear software platform and payment card environment and security system in a timely manner and to timely act upon warnings and alerts, including those generated by their own security systems.

99. Defendants owed a duty to Plaintiffs and Class Members to provide security consistent with industry standards and requirements and to ensure that the Blue Bear software platform and payment card environment, computer systems and networks—and the personnel responsible for them—adequately protected the Personal Information of Plaintiffs and Class Members whose confidential data Defendants processed, obtained and/or maintained.

100. Defendants owed the Plaintiffs and Class Members an independent duty of care to safeguard their personal information. "It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information[.]" In re Equifax, Inc., 362 F.Supp.3d 1295, 1321 (N.D. Ga. 2019).

101. Defendants knew, or should have known, of the risks inherent in collecting and storing Plaintiffs' and Class Members' Personal Information and the critical importance of providing adequate security for that information.

102. Defendants' conduct created a foreseeable risk of harm to Plaintiffs and Class Members. This conduct included but was not limited to Defendants' failure to take the steps and opportunities to prevent and stop the Data Breach as described herein. Defendants' conduct also included decisions not to comply with industry standards for the safekeeping and maintenance of the Personal Information of Plaintiffs and Class Members.

103. Defendants knew or should have known that they had inadequate software, computer systems and data security practices to safeguard such information, and Defendants knew or should have known that hackers would attempt or were attempting to access the personal financial collected and stored by Defendants.

104. Defendants breached the duties they owed to Plaintiffs and Class Members by failing to exercise reasonable care and implement adequate software, security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiffs and Class Members, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiffs and Class Members.

105. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made via Defendants' Blue Bear software platform and payment card environment that Plaintiffs and Class Members would not have made had they known of Defendants' careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances and bounced transactions; harm resulting from damaged credit scores and information; increased risk of future fraud and identity theft; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Personal Information, entitling them to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*

106. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

107. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate software, computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

108. 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 Defendants, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also form part of the basis of Defendants' duty to protect Plaintiffs' and Class Members' sensitive information.

109. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers and financial institutions.

110. Plaintiffs and Class Members are within the class of persons intended to be protected by the FTC Act and the harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

111. Defendants had a duty to Plaintiffs and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Personal Information.

112. Defendants owed the Plaintiffs and Class Members an independent duty of care to safeguard their personal information. "It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information[.]" In re Equifax, Inc., 362 F.Supp.3d 1295, 1321 (N.D. Ga. 2019).

113. Defendants breached their duties to Plaintiffs and Class Members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate software, computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

114. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) and their failure to comply with applicable laws and regulations constitute negligence *per se*.

115. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, they would not have been injured.

116. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the exposure of their Personal Information.

117. Had Plaintiffs and Class Members known that Defendants did and do not adequately protect customer Personal Information, they would not have made purchases via Defendants' Blue Bear software platform and payment card environment.

118. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made via Defendants' Blue Bear software platform and payment card environment that Plaintiffs and Class

Members would not have made had they known of Defendants' careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances and bounced transactions; harm resulting from damaged credit scores and information; increased risk of future fraud and identity theft; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Personal Information, entitling them to damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT

119. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

120. Plaintiffs and Class Members who made purchases via Defendants' Blue Bear software platform and payment card environment during the period in which the Data Breach occurred had implied contracts with Defendants.

121. Specifically, Plaintiffs and Class Members paid money via Defendants' Blue Bear software platform and payment card environment and, in connection with those transactions, provided Defendants with their Personal Information. In exchange, Defendants agreed, among other things: (1) to accept payments via the Blue Bear software platform and payment card environment for a fee; (2) to take

reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' Personal Information; and (3) to protect Plaintiffs' and Class Members' personal information in compliance with federal and state laws and regulations and industry standards.

122. Protection of personal information is a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Defendants, on the other hand. Indeed, as set forth, *supra*, Defendants recognized the importance of data security and privacy of consumers' sensitive financial information. Had Plaintiffs and Class Members known that Defendants would not adequately protect their Personal Information, they would not have made purchases via Defendants' Blue Bear software platform and payment card environment.

123. Defendants did not satisfy their promises and obligations to Plaintiffs and Class Members under the implied contracts because they did not take reasonable measures to keep the Personal Information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

124. Defendants materially breached their implied contracts with Plaintiffs and Class Members by failing to implement adequate payment card and Personal Information security measures.

125. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendants.

126. Defendants' failure to satisfy their obligations led directly to the successful intrusion of Defendants' software and computer systems and stored Personal Information and led directly to unauthorized parties access and exfiltration of Plaintiffs' and Class Members' Personal Information.

127. Defendants breached these implied contracts as a result of their failure to implement adequate security measures.

128. Also, as a result of Defendants' failure to implement the security measures, Plaintiffs and Class Members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

129. Accordingly, Plaintiffs and Class Members have been injured as a proximate result of Defendants breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD-PARTY BENEFICIARIES

130. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

131. Upon information and belief, Plaintiffs and Class Members are intended third-party beneficiaries of contracts entered into between Defendants and various entities including, without limitation, (i) contracts between Defendants and their merchant customers to process credit card and/or debit card transactions, (ii) contracts between Defendants and Visa and/or MasterCard (including their operating regulations), and (iii) contracts between Defendants and their acquiring banks.

132. Upon further information and belief, these contracts and regulations require, *inter alia*, that Defendants take appropriate steps to safeguard the sensitive financial information of Defendants' customers, like Plaintiffs and Class Members.

133. Plaintiffs and the Class Members are intended third party beneficiaries of these contracts and regulations. Under the circumstances, recognition of a right to performance by Plaintiffs and the Class Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiffs and the Class Members the benefit of the performance promised in the contracts.

134. Defendants breached these agreements, which directly and/or proximately caused Plaintiffs and the Class Members to suffer substantial damages.

135. Upon further information and belief, Defendants saved (or avoided spending) a substantial sum of money by knowingly failing to comply with their contractual obligations, and continues to do so.

136. Accordingly, Plaintiffs and Class Members who have been injured are entitled to damages, restitution, and other relief in an amount to be proven at trial.

COUNT V
VIOLATION OF THE UTAH CONSUMER SALES PRACTICES ACT
Utah Code Ann. § 13-11-4
(On Behalf of Plaintiff Blake and the Utah Class)

137. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

138. Utah Code Ann. § 13-11-4(1) provides:

> A deceptive act or practice by a supplier in connection with a consumer transaction violates this chapter whether it occurs before, during, or after the transaction.

139. Utah Code Ann. § 13-11-4(2) provides in part:

> Without limiting the scope of Subsection (1), a supplier commits a deceptive act or practice if the supplier knowingly or intentionally:
>
> ***
>
> (a) indicates that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not;

> (b) indicates that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;
>
> ***
>
> (i) indicates that the supplier has a sponsorship, approval, or affiliation the supplier does not have;

140. Utah Code Ann. § 13-11-2 provides in part:

> This act shall be construed liberally to promote the following policies:
>
> ***
>
> (4) to make state regulation of consumer sales practices not inconsistent with the policies of the Federal Trade Commission Act relating to consumer protection;

141. Plaintiff Blake and Utah Class Members are "persons" as defined by Utah Code Ann. § 13-11-3(5).

142. Defendants are "suppliers" as defined by Utah Code Ann. § 13-11-3(6).

143. The payments made by Plaintiff Blake and Utah Class Members via Defendants' Blue Bear software platform and payment card environment were "consumer transactions" as defined by Utah Code Ann. § 13-11-3(2)(a).

144. As noted above, the FTC and federal courts interpreting Section 5(a) of the Federal Trade Commission Act have concluded that failing to employ reasonable and appropriate measures to protect against unauthorized access to confidential

consumer data and overstating a business's cybersecurity through misleading privacy policies constitute unfair acts or practices prohibited by 15 U.S.C. § 45(a). *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3d Cir. 2015); *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

145. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Personal Information of Plaintiff Blake and the Utah Class Members, Defendants violated the above stated provisions of Utah Code Ann. § 13-11-4.

146. The acts and conduct of Defendants as alleged above violated the above stated provisions of Utah Code Ann. § 13-11-4 by, among other things:

- failing to maintain sufficient security to keep confidential and sensitive financial information of Plaintiff Blake and the Utah Class Members from being hacked and exfiltrated;

- misrepresenting material facts to Plaintiff Blake and the Utah Class Members, in connection with the sale of goods and providing online purchases services, by representing that Defendants would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Blake's and Utah Class Members' Personal Information from unauthorized disclosure, release, data breaches, and exfiltration;

- misrepresenting material facts to Plaintiff Blake and the Utah Class Members, in connection with the sale of goods and providing online purchases services, by representing

that Defendants did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff Blake's and Utah Class Members' Personal Information; and,

- failing to prevent the Data Breach and promptly notify consumers thereof, failing to maintain the privacy and security of Plaintiff Blake's and Utah Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws.

147. Due to the Data Breach, Plaintiff Blake and Utah Class Members have lost property in the form of their Personal Information and have suffered actual damages. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive financial information of their customers has resulted in Plaintiff Blake and Utah Class Members spending time and money to protect against identity theft. Plaintiff Blake and Utah Class Members are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

148. As a result of Defendants' practices, Plaintiff Blake and Utah Class Members have suffered injury-in-fact and have lost money or property. As a result of Defendants' failure to adopt, implement, and maintain reasonable security

procedures, and the resulting Data Breach, Plaintiff Blake and Utah Class Members have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

149. Plaintiff Blake and Utah Class Members seek all remedies available under Utah law.

COUNT VI
VIOLATION OF NEVADA'S DECEPTIVE TRADE PRACTICES ACT
Nev. Rev. Stat. Ann. § 598.0915
(On Behalf of Plaintiff Harrison and the Nevada Class)

150. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

151. Nev. Rev. Stat. Ann. § 598.0915 provides in part:

> A person engages in a "deceptive trade practice" if, in the course of his or her business or occupation, he or she:
>
> ***
>
> 2. Knowingly makes a false representation as to the source, sponsorship, approval or certification of goods or services for sale or lease.
>
> ***
>
> 5. Knowingly makes a false representation as to the characteristics, ingredients, uses, benefits, alterations or quantities of goods or services for sale or lease or a false representation as to the sponsorship, approval, status, affiliation or connection of a person therewith.

***

> 15. Knowingly makes any other false representation in a transaction.

152. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Personal Information of Plaintiff Harrison and the Nevada Class Members, Defendants violated the above stated provisions of Nev. Rev. Stat. Ann. § 598.0915.

153. The acts and conduct of Defendants as alleged above violated the above stated provisions of Nev. Rev. Stat. Ann. § 598.0915 by, among other things:

- failing to maintain sufficient security to keep confidential and sensitive financial information of Plaintiff Harrison and the Nevada Class Members from being hacked and exfiltrated;

- misrepresenting material facts to Plaintiff Harrison and the Nevada Class Members, in connection with the sale of goods and providing online purchases services, by representing that Defendants would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Harrison's and Nevada Class Members' Personal Information from unauthorized disclosure, release, data breaches, and exfiltration;

- misrepresenting material facts to Plaintiff Harrison and the Nevada Class Members, in connection with the sale of goods and providing online purchases services, by representing that Defendants did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff

Harrison's and Nevada Class Members' Personal Information; and,

- failing to prevent the Data Breach and promptly notify consumers thereof, failing to maintain the privacy and security of Plaintiff Harrison's and Nevada Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws.

154. Due to the Data Breach, Plaintiff Harrison and Nevada Class Members have lost property in the form of their Personal Information and have suffered actual damages. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive financial information of their customers has resulted in Plaintiff Harrison and Nevada Class Members spending time and money to protect against identity theft. Plaintiff Harrison and Nevada Class Members are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

155. As a result of Defendants' practices, Plaintiff Harrison and Nevada Class Members have suffered injury-in-fact and have lost money or property. As a result of Defendants' failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Plaintiff Harrison and Nevada Class

Members have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

156. Plaintiff Harrison and Nevada Class Members seek all remedies available under Nevada law.

COUNT VII
VIOLATION OF GEORGIA'S DATA BREACH NOTIFICATION STATUTE, Ga. Code Ann. § 10-1-910 *et seq.*
(On Behalf of All Plaintiffs and the National Class)

157. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

158. Ga. Code Ann. § 10-1-910 provides:

> The General Assembly finds and declares as follows:
>
> (1) The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sectors;
>
> (2) Credit card transactions, magazine subscriptions, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet websites are all sources of personal information and form the source material for identity thieves;
>
> (3) Identity theft is one of the fastest growing crimes committed in this state. Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, purchase property, and commit other financial crimes with other people's identities;

> (4) Implementation of technology security plans and security software as part of an information security policy may provide protection to consumers and the general public from identity thieves;
>
> (5) Information brokers should clearly define the standards for authorized users of its data so that a breach by an unauthorized user is easily identifiable;
>
> (6) Identity theft is costly to the marketplace and to consumers; and
>
> (7) Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of unauthorized acquisition and possible misuse of a person's personal information is imperative.

159. Defendants are "information brokers" as defined by Ga. Code Ann. § 10-1-911(3).

160. Defendants are "persons" as defined by Ga. Code Ann. § 10-1-911(5).

161. The Data Breach was a "breach of the security of the system" as defined by Ga. Code Ann. § 10-1-911(1).

162. Plaintiffs' and Class Members' Personal Information compromised in the Data Breach was "personal information" as defined by Ga. Code Ann. § 10-1-911(5).

163. The Data Breach constituted a security breach that triggered the notice provisions of Ga. Code Ann. § 10-1-910 *et seq.* and the Personal Information taken

includes categories of personal information protected by Ga. Code Ann. § 10-1-910 *et seq*.

164. Defendants unreasonably delayed in informing Plaintiffs and Class Members, about the Data Breach after Defendants knew or should have known that the Data Breach had occurred.

165. Had Defendants provided timely and accurate notice, Plaintiffs and Class Members could have avoided or mitigated the harm caused by the Data Breach. For example, they could have contacted their banks to cancel any affected cards, taken security precautions in time to prevent or minimize identity theft, or could have avoided using uncompromised payment cards during subsequent purchases via the Blue Bear software platform and payment card environment.

166. Defendants' failure to provide timely and accurate notice of the Data Breach violated Ga. Code Ann. § 10-1-912.

167. Plaintiffs and Class Members were damaged by Defendants' failure to comply with Georgia's data breach notification statute.

168. Plaintiffs and Class Members seek all remedies available under Georgia law.

COUNT VIII
UNJUST ENRICHMENT

169. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

170. This claim is plead in the alternative to the above breach of contract claims.

171. Plaintiffs and Class Members conferred a monetary benefit upon Defendants in the form of fees Defendants collected for processing payments Plaintiffs and Class Members made via Defendants' Blue Bear software platform and payment card environment.

172. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. Defendants also benefited from the receipt of Plaintiffs' and Class Members' Personal Information, as this was utilized by Defendants to facilitate payments.

173. The monies collected by Defendants in exchange for processing payments via Defendants' Blue Bear software platform and payment card environment were supposed to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

174. Defendants failed to provide reasonable data privacy and security practices and procedures for the Blue Bear software platform and payment card environment.

175. As a result of Defendants' conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

176. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

177. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23(a) and (b), and, pursuant to Fed. R. Civ. P. 23(g), appoint Plaintiffs as Class representatives and their counsel as Class counsel.

B. Award Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement.

C. Award Plaintiffs and the Class equitable, injunctive, and declaratory relief as may be appropriate. Plaintiffs, on behalf of the Class, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard consumers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly Class Members who are more susceptible to fraud and identity theft.

D. Award Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity.

Dated: April 13, 2020

Respectfully submitted,

/s/ Andrea S. Hirsch
Andrea Hirsch (GA Bar No. 666557)
THE HIRSCH LAW FIRM
230 Peachtree Street, Suite 2260
Atlanta, Georgia 30303
Telephone: 404-487-6552
Facsimile: 678-541-9356
andrea@thehirschlawfirm.com

Tina Wolfson (CA Bar No. 174806)
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
310.474.9111 (telephone)
310.474.8585 (facsimile)
twolfson@ahdootwolfson.com

Cornelius P. Dukelow (OK Bar No. 19086)
ABINGTON COLE + ELLERY
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (telephone & facsimile)
cdukelow@abingtonlaw.com

Counsel for Plaintiffs and the Putative Classes

JS44 (Rev. 6/2017 NDGA)

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

BRIAN H. BLAKE and CATHERINE HARRISON individually and on behalf of all others similarly situated

DEFENDANT(S)

GLOBAL PAYMENTS INC., a Georgia corporation and ACTIVE NETWORK, LLC, a Delaware limited liability company

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Salt Lake, Utah
(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

The Hirsch Law Firm
230 Peachtree Street, NW, Suite 2260
Atlanta, Georgia 30303
404-487-6552
andrea@thehirschlawfirm.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ☐ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☑ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☑ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. ORIGIN (PLACE AN "X "IN ONE BOX ONLY)

- ☑ 1 ORIGINAL PROCEEDING
- ☐ 2 REMOVED FROM STATE COURT
- ☐ 3 REMANDED FROM APPELLATE COURT
- ☐ 4 REINSTATED OR REOPENED
- ☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Class action with diversity (28 U.S.C. § 1332(d)); allegations include negligence, negligence per se, breach of implied contract, breach of contract (third-party beneficiary), Utah Consumer Sales Practices Act (Utah Code Ann. § 13-11-4), Nevada Deceptive Trade Practices Act (Nev. Rev. Stat. Ann. § 598.0915), Georgia Data Breach Notification Statute (Ga. Code Ann. § 10-1-910 et seq.), and unjust enrichment stemming from a data breach.

(IF COMPLEX, CHECK REASON BELOW)

- ☐ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☐ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☑ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** over $5,000,000.00

JURY DEMAND ☑ **YES** ☐ **NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE_____ **DOCKET NO.**_____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)
- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

Andrea S. Hirsch — April 13, 2020

SIGNATURE OF ATTORNEY OF RECORD **DATE**