IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CRYSTAL BRAY and SAMUEL COOK, on behalf of themselves and all others similarly situated,	)	CASE NO.
Plaintiffs,	)	**CLASS ACTION COMPLAINT**
v.	)	
GAMESTOP CORPORATION,	)	
Defendant.	)	**JURY TRIAL DEMANDED**

Plaintiffs Crystal Bray and Samuel Cook ("Plaintiffs") individually and on behalf of all others similarly situated, allege the following against Defendant GameStop Corporation ("GameStop" or "Defendant") based on personal knowledge as to their own experiences and upon information and belief 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, addresses, and credit card and debit card numbers, expiration dates, security information, and other card information (collectively, "Card Information") was compromised in a massive security breach of Defendant's computer servers beginning on or around August 10, 2016 and lasting until February 9, 2017 (the "Data Breach").

2. As alleged herein, Defendant's failure to implement or maintain adequate data security measures for customer information, including Card Information, directly and proximately caused injuries to Plaintiffs and the Class.

3. Defendant failed to take reasonable steps to employ adequate security measures or to properly protect sensitive payment Card Information despite well-publicized data breaches at large national retail and restaurant chains in recent years, including Arby's, Wendy's, Target, Chipotle, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Dairy Queen, and Kmart.

4. The Data Breach was the inevitable result of GameStop's inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and despite the fact that these types of data breaches were and are occurring throughout the restaurant and retail industries, GameStop failed to ensure that it maintained adequate data security measures causing customer Card Information to be stolen.

5. As a direct and proximate consequence of Defendant's negligence, a massive amount of customer information was stolen from GameStop. Upon information and belief, the GameStop Data Breach compromised the Card Information of thousands (if not more) of GameStop customers. Victims of the Data Breach have had their Card Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft (with many consumers actually having suffered incidents of fraud or identity theft), lost control over their personal and financial information, and otherwise been injured.

6. 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, and/or other losses resulting from the unauthorized use of their cards or accounts.

7. Rather than providing meaningful assistance to consumers to help deal with the fraud that has and will continue to result from the Data Breach, GameStop simply tells them to carefully monitor their accounts. In contrast to what is and has been frequently made available to consumers in recent data breaches, GameStop has not offered or provided any monitoring service or fraud insurance to date.

8. Plaintiffs and Class Members seek to recover damages caused by Defendant's negligence, negligence *per se*, breach of contract, and violations of state consumer protection statutes. Additionally, Plaintiffs seek declaratory and injunctive relief as a result of the conduct of Defendant discussed herein.

PARTIES

Plaintiff Crystal Bray

9. Plaintiff Crystal Bray is an adult residing in Fayetteville, North Carolina. On or about February 2, 2017, Plaintiff Bray used her United Services Automobile Association Federal Savings Bank ("USAA") debit card to make a purchase in the amount of $283.74 from www.GameStop.com. Plaintiff Bray's purchase included an Xbox One system, controller, and two video games.

10. Plaintiff Bray's USAA debit card is tied to a checking account where her husband's Veterans Administration Disability pay is deposited. These are the primary funds with which Plaintiff Bray's family is supported.

11. In early June 2017, Plaintiff Bray received a letter from GameStop informing that it had become aware of "a security incident that may have involved [Plaintiff Bray's] payment card information" and that "data from payment cards used on www.GameStop.com may have been obtained by unauthorized individuals." The information potentially obtained by an

unauthorized third-party "may" have included Plaintiff Bray's name, address, payment card number, card expiration date, and Card Verification Value ("CVV"). Although the letter was dated June 2, 2017, it indicated GameStop determined the potential for customers' information to have been stolen nearly two months before, on April 18, 2017. The letter did not offer any credit monitoring, compensation, identity theft insurance coverage, or other remedy for losses.

12. On June 13, 2017, Plaintiff Bray received an email notification from USAA that her account balance was $0. Upon immediately checking the transaction history of her banking account online, Plaintiff Bray discovered that a fraudulent charge had been made on her account. This charge was in the amount of $811.84 and made at a Home Depot in San Jose, California on June 14, 2017.

13. The card used to make the fraudulent charge was the same as that used by Plaintiff Bray on www.GameStop.com on February 2, 2017.

14. That same day, Plaintiff Bray contacted USAA and notified the bank of the fraudulent charge to her account. USAA promptly cancelled the debit cards associated with all of Plaintiff Bray's checking accounts and mailed her new debit cards.

15. While Plaintiff Bray waited for the new debit cards, she had to utilize a credit card to pay for her family's necessities. She also had to contact several bill holders, including her car insurance and renter's insurance companies, to request her billing due dates be postponed.

16. After discovering the fraudulent charges, Plaintiff Bray called GameStop, but the representative with whom she spoke offered no remedy or compensation for Plaintiff Bray's lost time, compromised information, financial difficulties, or loss of control over her personal information.

17. Prior to the May 10, 2017, fraudulent transaction, Plaintiff Bray had not experienced credit card fraud or identity theft with respect to her debit card. Furthermore, Plaintiff Bray does not have a previous history of being victimized by payment card fraud.

18. Although Plaintiff Bray was ultimately refunded her stolen money, as a result of having been victimized by the GameStop Data Breach, Plaintiff Bray was required to spend a significant amount of time—at least seven hours—addressing the unauthorized transactions.

19. Had Plaintiff Bray known that GameStop would not adequately protect the Card Information and other sensitive information entrusted to it, she would not have made a purchase at www.GameStop.com using her debit card.

20. As a result of GameStop's failure to adequately safeguard Plaintiff Bray's Card Information, Plaintiff Bray has been injured.

Plaintiff Samuel Cook

21. Plaintiff Samuel Cook is an adult residing in Indianapolis, Indiana. On or about October 5, 2016, Plaintiff Cook used his Citi branded Visa credit card to make a purchase in the amount of $85.59 from www.GameStop.com.

22. In early June 2017, Plaintiff Cook received a letter from GameStop. The letter informed Plaintiff Cook that GameStop had become aware of "a security incident that may have involved [Plaintiff Cook's] payment card information" and that "data from payment cards used on www.GameStop.com may have been obtained by unauthorized individuals." Information potentially obtained by an unauthorized third-party "may" have included Plaintiff Cook's name, address, payment card number, card expiration date, and CVV. Although the letter was dated June 2, 2017, it indicated that GameStop determined the potential for customers' information to

have been stolen nearly two months before on April 18, 2017. The letter did not offer customers any credit monitoring, compensation, or other remedy for losses.

23. Shortly after receiving the letter from GameStop, Plaintiff Cook accessed his credit card account online. While reviewing the most recent transactions for his Citi Visa credit card—the card he used to make purchases on GameStop.com—Plaintiff Cook noticed approximately 20 fraudulent charges for Domino's Pizza and LYFT rides from May 28, 2017, through June 1, 2017. These fraudulent charges totaled $487.76.

24. Plaintiff Cook called and notified Citi customer service of the fraudulent charges. On or about July 7, 2017, Citi refunded the fraudulent charges.

25. After receiving the letter from GameStop, Plaintiff Cook reviewed in more detail previous credit card statements for his Citi card. After reviewing his April 26 to May 23, 2017, credit card statement, he noticed a fraudulent charge from North 40 Outfitters dated May 1, 2017, in the amount of $6,359.98, and a corresponding credit in the same amount of $6,359.98 dated May 8, 2017.

26. Prior to these fraudulent transactions, Plaintiff Cook had not experienced credit card fraud or identity theft with respect to his Citi card. Furthermore, Plaintiff Cook does not have a previous history of being victimized by payment card fraud.

27. As a result of being victimized by the Data Breach, Plaintiff Cook was required to spend a significant amount of time—approximately three to four hours—addressing the unauthorized transactions and updating bill payments.

28. Had Plaintiff Cook known that GameStop does not adequately protect Card Information and other sensitive information, he would not have made a purchase at

www.GameStop.com. As a result of GameStop's failure to adequately safeguard Plaintiff Cook's Card Information, Plaintiff Cook has been injured.

Defendant

29. Defendant GameStop Corporation is a Delaware corporation with a principal executive office located at 625 Westport Parkway, Grapevine, Texas. GameStop operates a chain of approximately 7,500 retail stores worldwide. Additionally, its online consumer product network includes www.GameStop.com, www.Kongregate.com, and www.ThinkGeek.com.[1] In its 2017 fiscal year, GameStop's revenues totaled approximately $8.6 billion.[2]

JURISDICTION AND VENUE

30. 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 Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

31. This Court has personal jurisdiction over Defendant. GameStop, a Delaware Corporation, has sufficient minimum contacts with the state of Delaware and intentionally avails itself of the consumers and markets within the state through the promotion, marketing, and sale of its products.

32. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because Defendant incorporated in and conducts substantial business in this district, and is deemed to be

[1] Tom Spring, *GameStop Online Shoppers Officially Warned of Breach*, THREATPOST (June 9, 2017, 4:11 PM), https://threatpost.com/gamestop-online-shoppers-officially-warned-of-breach/126172/.

[2] NASDAQ, *GameStop Corporation Revenue & Earnings Per Share (EPS)*, http://www.nasdaq.com/symbol/gme/revenue-eps (last visited July 13, 2017).

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

FACTUAL ALLEGATIONS

The GameStop Data Breach

33. As early as April 7, 2017, Defendant confirmed to media outlets that it was investigating a possible data breach that compromised customers' Card Information between September 2016 and February 2017.[3] Financial industry sources claimed that the breach included not only card numbers, expiration dates and cardholder addresses, but also the three-digit CVV security number that is ordinarily difficult to obtain in a data breach because the CVV is not usually stored online.[4] Some outlets posited that the compromise of CVVs suggested the hackers planted malware on the site to harvest the information before it was transmitted.[5] GameStop told media outlets that its customers' payment data may have been "offered for sale on a website."[6]

34. It was not until nearly two months later, in a letter dated June 2, 2017 that GameStop notified customers of the Data Breach. The letter informed customers GameStop had become aware of "a security incident that may have involved . . . payment card information" and that "data from payment cards used on www.GameStop.com may have been obtained by unauthorized individuals." It went on to state that information potentially obtained by an unauthorized third-party "may" have included customers' names, addresses, payment card

[3] *See, e.g.*, KREBS ON SECURITY, *GameStop.com Investigating Possible Data Breach* (Apr. 7, 2017), https://krebsonsecurity.com/2017/04/gamestop-com-investigating-possible-breach/ (reporting that a GameStop spokesman stated that GameStop had "engaged" a leading security firm to investigate the Data Breach); John Fingas, *GameStop Looks Into a Potentially Serious Credit Card Breach*, ENGADGET (Apr. 9, 2017), https://www.engadget.com/2017/04/09/gamestop-credit-card-breach/.
[4] *Id.*
[5] *Id.*
[6] *Id.*

numbers, card expiration dates, and CVVs. The letter did not offer customers any credit monitoring, compensation, or other remedy for losses.

35. The letter also stated that GameStop determined on April 18, 2017, that there was the potential for a data breach of Defendant's system. That date is nearly 10 days after media outlets began reporting that GameStop was aware of the potential for a data breach.[7] Upon information and belief, GameStop did not notify customers prior to June 2, 2017. Outlets called the timing "pretty troubling"[8] and noted "it's safe to say many people were exposed."[9]

36. An undated "SECURITY UPDATE" on Defendant's website indicates that GameStop became aware of the Data Breach after being notified by a third party that "payment card data from cards used on the GameStop.com website was being offered for sale on a website."[10]

37. Neither the letter, the statement on Defendant's website, nor the contemporaneous statements by GameStop to media outlets gave any indication as to the magnitude of the Data Breach or the number of customers affected. However, the Data Breach time period in which customers' Card Information was compromised included the 2016 back-to-school and holiday seasons—times of year when retailers typically experience a high volume of sales.

38. GameStop's website accepts customer payment cards for the purchase of products. Upon information and belief, the GameStop Data Breach affected the large majority of

---

[7] John Fingas, *GameStop Looks Into a Potentially Serious Credit Card Breach*, ENGADGET (Apr. 9, 2017), https://www.engadget.com/2017/04/09/gamestop-credit-card-breach/.
[8] Dan O'Shea, *GameStop E-commerce Site 'Likely' Hacked, Card Data Potentially Stolen*, RETAIL DIVE (Apr. 9, 2017), http://www.retaildive.com/news/gamestop-e-commerce-site-likely-hacked-card-data-potentially-stolen/440085/.
[9] Mallory Locklear, *GameStop Confirms Extensive Credit Card Data Breach*, ENGADGET (June 9, 2017), https://www.engadget.com/2017/06/09/gamestop-confirms-credit-card-data-breach/.
[10] GAMESTOP, *Security Update*, http://www.gamestop.com/securityupdate (last visited July 17, 2017).

credit and debit cards used to purchase goods on www.GameStop.com during the vulnerable time period.

Industry Standards and the Protection of Customer Card Information

39. It is well known that customer Card Information is valuable and frequently targeted by hackers. Despite the risk of a data breach and the widespread publicity and industry alerts regarding the other notable data breaches, GameStop failed to take reasonable steps to adequately protect its computer systems from being breached.

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

41. GameStop's privacy policy acknowledges that customers expect it to adequately safeguard their Card Information: "GameStop knows that you care about your privacy and the use of your personal information."[11]

42. GameStop is, and at all relevant times has been, aware of the importance of safeguarding its customers' Card Information and of the foreseeable consequences that would occur if its data security systems were breached.

43. 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.

44. 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

[11] GAMESTOP, *Privacy Policy*, https://www.gamestop.com/gs/help/PrivacyPolicy.aspx (last visited Sept. 26, 2017) (privacy policy in place since August 26, 2015).

where cardholder data is stored, processed, or transmitted, and requires merchants like Defendant to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

45. 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.[12]

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

47. Defendant was at all times fully aware of its data protection obligations for GameStop stores in light of its participation in the payment card processing networks and the stores daily collection and transmission of tens of thousands of sets of Card Information.

48. Because www.GameStop.com accepted payment cards containing sensitive financial information, Defendant knew that its customers were entitled to, and did, rely on

[12] 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=1506536983345.

Defendant to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

49. 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 Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

50. 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.

51. 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.[13]

[13] FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), www.stopfraudcolorado.gov/sites/default/files/bus69-protecting-personalinformation-guide-business_0.pdf.

52. 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.

53. As noted above, Defendant should have been aware of the need to have adequate data security systems in place.

54. Despite this, GameStop failed to upgrade and maintain its data security systems in a meaningful way so as to prevent data breaches. Had GameStop maintained its information technology ("IT") systems and adequately protected them, it could have prevented the Data Breach.

55. GameStop's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at GameStop are in stark contrast and directly conflict with the PCI DSS core security standards. Had GameStop had adequate security safeguards in place, the Data Breach would not have occurred.

56. 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.

57. 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 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.

58. In addition to the publicly announced data breaches described above, 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 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.[14]

59. Despite the fact that Defendant was on notice of the very real possibility of consumer data theft associated with its security practices and that Defendant knew or should have known about the elementary infirmities associated with GameStop's security systems, it still failed to make necessary changes to its security practices and protocols.

60. Defendant, at all times relevant to this action, had a duty to Plaintiffs and members of the Class to: (a) properly secure Card Information submitted to or collected on Defendant's website and on Defendant's internal networks; (b) encrypt Card Information using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiffs and the Class, which would naturally result from Card Information theft; and (e) promptly notify customers when Defendant became aware of the potential that customers' Card Information may have been compromised.

61. Defendant negligently allowed Card Information to be compromised by failing to take reasonable steps against an obvious threat.

62. In addition, leading up to the GameStop Data Breach, and during the course of the breach itself and the investigation that followed, GameStop failed to follow the guidelines set forth by the FTC. Indeed, Julie Conroy—research director at the research and advisory firm Aite

[14] *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.

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.[15]

63. As a result of the events detailed herein, Plaintiffs and members of the Class suffered losses resulting from the GameStop Data Breach, 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 at GameStop that Plaintiffs and Class members would not have made had they known of GameStop's 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; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

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

65. The information stolen from GameStop's website can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.

66. Even if credit card companies may be responsible for or reimburse some of the unauthorized transactions, consumers affected by the Data Breach may be liable for fraudulent charges below a threshold $50 amount.[16]

67. To date, GameStop does not appear to be taking any measures to assist affected customers other than telling them to simply do the following:

---

[15] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017, 2:39 PM), http://www.reuters.com/article/us-Chipotle-cyber-idUSKBN18M2BY.

[16] *See, e.g.*, WHEC, *Local Couple Impacted by Chipotle Data Breach* (May 31, 2017, 8:09 PM), http://www.whec.com/news/restaurants-exposed-local-couple-Chipotle-breach/4500701/.

- review financial statements;
- report unauthorized charges to financial institutions;
- obtain a copy of credit reports; and
- contact the FTC and/or the state Attorney General's office.

68. GameStop's failure to adequately protect consumers' Card Information has resulted in consumers having to undertake these errands that require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money—while GameStop is not doing anything to assist those affected by the data breach. Instead, as one source identified, GameStop is putting the burden on the consumer to discover possible fraudulent transactions.

CLASS ALLEGATIONS

69. Plaintiffs bring this action on their own behalf, and on behalf of the following Class pursuant to FED. R. CIV. P. 23:

> All GameStop customers who used a credit or debit card to place (or attempted to place) a purchase on www.GameStop.com between August 10, 2016 and February 9, 2017.

70. In the alternative, Plaintiffs seek to represent the following state classes:

Indiana Class

> All GameStop customers who used a credit or debit card to place (or attempted to place) a purchase on www.GameStop.com between August 10, 2016 and February 9, 2017 and whose non-public information was compromised in the Data Breach.

North Carolina Class

> All GameStop customers who used a credit or debit card in North Carolina to place (or attempted to place) a purchase on www.GameStop.com between August 10, 2016 and February 9, 2017 and whose non-public information was compromised in the Data Breach.

71. The above classes are collectively referred to as the "Class." Excluded from the Class are Defendant, its 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 Class based on discovery and further investigation.

72. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include many thousands of members who are geographically dispersed. Upon information and belief, the Data Breach affected people across the United States.

73. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through GameStop's 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 member of the Class had their data and Card Information compromised in the same way by the same conduct by GameStop.

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

75. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. 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 members of the Class individually to effectively redress Defendant's 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.

76. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to plaintiffs and all members of the Class. 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 GameStop engaged in the wrongful conduct alleged herein;
- whether GameStop owed a duty to Plaintiffs and members of the Class to adequately protect their Card Information and to provide timely and accurate notice of the data breach to Plaintiffs and the Class, and whether it breached these duties;
- whether GameStop violated federal and state laws thereby breaching its duties to Plaintiffs and the Class;
- whether GameStop knew or should have known that its computer and network systems were vulnerable to attack from hackers;
- whether GameStop's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems resulting in the loss of customers' Card Information;
- whether GameStop wrongfully failed to inform Plaintiffs and members of the Class

that it did not maintain computer software and other security procedures sufficient to reasonably safeguard consumer financial and personal data.

- whether GameStop failed to inform Plaintiffs and the Class of the data breach in a timely and accurate manner;
- whether GameStop wrongfully waited to inform Plaintiffs and Class members that their sensitive financial and personal information was exposed in the security breach;
- whether GameStop continues to breach duties to Plaintiffs and Class;
- whether GameStop has sufficiently addressed, remedied, or protected Plaintiffs and Class members following the data breach and has taken adequate preventive and precautionary measures to ensure the Plaintiffs and Class members will not experience further harm;
- whether Plaintiffs and members of the Class suffered injury as a proximate result of GameStop's conduct or failure to act; and
- whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and the Class.

77. Defendant has acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Class as a whole.

78. Given that Defendant has engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law and statutory violations are involved and common questions far outweigh any potential individual questions.

79. The Class is defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Card Information to cyber criminals due to Defendant's failure to protect this information and adequately warn the Class that it was breached. Class membership will be readily ascertainable from Defendant's business records.

80. Plaintiffs reserve the right to revise the above Class definitions based on facts adduced in discovery.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

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

82. GameStop collected Card Information from Plaintiffs and Class Members in exchange for its sale of merchandise.

83. GameStop owed a duty to Plaintiffs and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in GameStop's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing GameStop's security systems to ensure that Plaintiffs' and Class members' financial and personal information in GameStop's possession was adequately protected both after collection and in the process of collection.

84. GameStop further owed a duty to Plaintiffs and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

85. GameStop owed a duty to Plaintiffs and Class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiffs and Class members whose confidential data GameStop obtained and maintained.

86. GameStop knew, or should have known, of the risks inherent in collecting and storing the financial and personal information of Plaintiffs and Class members and of the critical importance of providing adequate security for that information.

87. GameStop's conduct created a foreseeable risk of harm to Plaintiffs and members of the Class. This conduct included but was not limited to GameStop's failure to take the steps and opportunities to prevent and stop the Data Breach as described in this Complaint. GameStop's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiffs and Class members.

88. GameStop knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and GameStop knew or should have known that hackers were attempting to access the personal information in databases such as GameStop's.

89. GameStop breached the duties it owed to Plaintiffs and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiffs and members of the Class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiffs and Class members.

90. As a direct and proximate result of GameStop's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

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

92. Pursuant to the FTC Act, 15 U.S.C. § 45, GameStop had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' personal information.

93. 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 GameStop, of failing to use reasonable measures to protect Card Information. The FTC publications and orders described above also form part of the basis of GameStop's duty.

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

95. 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.

96. GameStop 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.

97. GameStop breached its duties to Plaintiffs and Class Members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' financial and personal information.

98. GameStop's violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

99. But for GameStop's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

100. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of GameStop's breach of its duties. GameStop knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the exposure of their Card Information.

101. Had Plaintiffs and Class Members known that GameStop did and does not adequately protect customer Card Information, they would not have made purchases at www.GameStop.com.

102. As a direct and proximate result of GameStop's negligence *per se*, Plaintiffs and Class Members have suffered harm, including but not limited to 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 at GameStop that Plaintiffs and Class members would not have made had they known of GameStop's 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; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Contract
(On Behalf of Plaintiffs and the Class)

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

104. Plaintiffs and Class Members who made or attempted to make purchases at www.GameStop.com during the period in which the Data Breach occurred had express contracts with GameStop.

105. Specifically, Plaintiffs and Class Members paid money to GameStop and, in connection with those transactions, provided GameStop with their Card Information. In exchange, GameStop agreed, among other things: (1) to provide products to Plaintiffs and Class Members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' Card Information; and (3) to protect Plaintiffs' and Class Members' personal information in compliance with federal and state laws and regulations and industry standards.

106. Protection of personal information is a material term of the contracts between Plaintiffs and Class Members, on the one hand, and GameStop, on the other hand. Had Plaintiffs and Class Members known that GameStop would not adequately protect customer Card Information, they would not have made purchases at www.GameStop.com.

107. GameStop did not satisfy its promises and obligations to Plaintiffs and Class Members under the express contracts because it did not take reasonable measures to keep Plaintiffs' and Class Members' personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

108. GameStop materially breached its express contracts with Plaintiffs and Class Members by failing to implement adequate payment card and Card Information security measures.

109. Plaintiffs and Class Members fully performed their obligations under their express contracts with GameStop.

110. GameStop's failure to satisfy its obligations led directly to the successful intrusion of GameStop's computer servers and stored Card Information and led directly to unauthorized parties access and exfiltration of Plaintiffs' and Class Members' Card Information.

111. GameStop breached these express contracts as a result of its failure to implement security measures.

112. Also, as a result of GameStop's 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.

113. Accordingly, Plaintiffs and Class Members have been injured as a proximate result of GameStop's breaches of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

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

115. Plaintiffs and Class Members who made or attempted to make purchases at www.GameStop.com during the period in which the Data Breach occurred had implied contracts with GameStop.

116. Specifically, Plaintiffs and Class Members paid money to GameStop and, in connection with those transactions, provided GameStop with their Card Information. In exchange, GameStop agreed, among other things: (1) to provide products to Plaintiffs and Class Members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' Card Information; and (3) to protect Plaintiffs' and Class Members' personal information in compliance with federal and state laws and regulations and industry standards.

117. Protection of personal information is a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and GameStop, on the other hand. Had Plaintiffs and Class Members known that GameStop would not adequately protect customer Card Information, they would not have made purchases at www.GameStop.com.

118. GameStop did not satisfy its promises and obligations to Plaintiffs and Class Members under the implied contracts because it did not take reasonable measures to keep

Plaintiffs' and Class Members' personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

119. GameStop materially breached its implied contracts with Plaintiffs and Class Members by failing to implement adequate payment card and Card Information security measures.

120. Plaintiffs and Class Members fully performed their obligations under their implied contracts with GameStop.

121. GameStop's failure to satisfy its obligations led directly to the successful intrusion of GameStop's computer servers and stored Card Information and led directly to unauthorized parties access and exfiltration of Plaintiffs' and Class Members' Card Information.

122. GameStop breached these implied contracts as a result of its failure to implement security measures.

123. Also, as a result of GameStop's 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.

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

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

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

126. This claim is plead in the alternative to the above contract claim.

127. Plaintiffs and Class Members conferred a monetary benefit upon GameStop in the form of monies paid for the purchase of products.

128. GameStop appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. GameStop also benefited from the receipt of Plaintiffs' and Class members' Card Information, as this was utilized by GameStop to facilitate payment to it.

129. The monies for products that Plaintiffs and Class Members paid to GameStop were supposed to be used by GameStop, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

130. As a result of GameStop's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between products with the reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for and the inadequate products without reasonable data privacy and security practices and procedures that they received.

131. Under principals of equity and good conscience, GameStop should not be permitted to retain the money belonging to Plaintiffs and Class Members because GameStop 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.

132. GameStop 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.

COUNT VI
Violation of the Indiana Deceptive Consumer Sales Act
IND. CODE §§ 24-5-0.5-1, *et seq.* ("IDCSA")
(On Behalf of Plaintiff Cook and the Indiana Class)

133. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

134. Defendant is a "supplier" who engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions," in violation of IDCSA, by engaging in (but not limited to) the following conduct:

- Failing to maintain sufficient security to keep Plaintiff's and Class Members' sensitive Card Information being hacked and stolen;
- Misrepresenting and fraudulently advertising (or omitting) material facts by representing and advertising that it would (or omitting that it would not) maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' financial and personal information from unauthorized disclosure, release, data breaches, and theft;
- Misrepresenting (or omitting) material facts to Plaintiff and the Class by representing and advertising that it did and would (or omitting that it would not) comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' financial and personal information;
- Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' financial and personal information;

- Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff's and Class Members' financial and personal information in violation of duties imposed by and public policies reflected in applicable federal and state laws resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and Indiana's data breach statute (IND. CODE § 24-4.9-3.5); and
- Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to Plaintiff and Class Members in a timely and accurate manner, contrary to the duties imposed by IND. CODE § 24-4.9-3.3.

135. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Class Members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their financial and personal information and damages.

136. The above unfair and deceptive practices and acts by Defendant were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under the IDCSA.

137. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' financial and personal information and that risk of a data breach or theft was highly likely.

138. Plaintiff Cook and Class Members seek relief under IND. CODE § 24-5-0.5-4, including, not limited to damages, restitution, penalties, injunctive relief, and/or attorneys' fees

and costs. Senior Members of the Class injured by Defendant's unfair and deceptive trade practices also seek treble damages pursuant to IND. CODE §24-5-0.5-4(i).

COUNT VII
Violation of the North Carolina Unfair and Deceptive Trade Practices Act, N.C. GEN. STAT. §§ 75-1.1, *et seq.* ("NCUDTPA")
(On Behalf of Plaintiff Bray and the North Carolina Class)

139. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

140. The NCUDTPA prohibits a person from engaging in "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]"

141. The NCUDTPA provides a private right of action for any person injured "by reason of any act or thing done by any other person, firm or corporation in violation of" the NCUDTPA. N.C. GEN. STAT. § 75-16.

142. Defendant's acts and practices complained of herein were performed in the course of Defendant's trade or business and thus occurred in or affected "commerce," as defined in N.C. GEN. STAT. § 75-1.1(b).

143. GameStop engaged in deceptive and unfair acts and practices, misrepresentation, and concealment, suppression, and omission of material facts in connection with the sale and advertisement of merchandise in violation of the NCUDTPA. Defendant's acts and practices are unfair and/or deceptive in at least the following respects:

- failing to maintain sufficient security to keep Plaintiff's and Class Members' sensitive Card Information being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of products, by representing that they would maintain adequate data privacy and

security practices and procedures to safeguard Class Members' Card Information from unauthorized disclosure, release, data breaches, and theft;

- misrepresenting material facts to the Class, in connection with sale of products, by representing that GameStop did and would (or omitting that it would not) comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' Card Information; and
- failing to take proper action following the data breach to enact adequate privacy and security measures and protect Class Members' Card Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

144. In addition, GameStop's failure to disclose that its computer systems were not well-protected and that Plaintiff's and Class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because GameStop knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Class; and (b) defeat Plaintiff's and Class members' ordinary, foreseeable, and reasonable expectations concerning the security of their Card Information on GameStop's computer servers.

145. Defendant intended that Plaintiff and the Class would rely on its deceptive and unfair acts and practices, misrepresentations, and concealment, suppression, and omission of material facts in connection with GameStop's offering of products and incorporating Plaintiff's and Class members' Card Information on its computer servers in violation of the NCUDTPA.

146. GameStop also engaged in unfair acts and practices in connection with the sale of services by failing to maintain the privacy and security of Class Members' personal information in violation of duties imposed by and public policies reflected in applicable federal and state laws resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and similar state laws.

147. Defendant's acts and practices are contrary to North Carolina law and policy and constitute immoral, unethical, oppressive, and unscrupulous business practices that caused substantial injury to Plaintiff and Class members. The gravity of the harm resulting from Defendant's unfair conduct outweighs any potential utility of the conduct. GameStop's wrongful practices were and are injurious to the public interest because those practices were part of a generalized, common, and uniform course of wrongful conduct on the part of GameStop that applied to all Class members and were repeated continuously before and after GameStop obtained sensitive Card Information and other information from Plaintiff and Class members. All Class members have been adversely affected by GameStop's conduct, and the public was and is at risk as a result thereof. There are reasonably available alternatives that would further Defendant's business interests of increasing sales and facilitating payment. Consumers could not reasonably avoid the harm from Defendant's unfair conduct.

148. As a result of GameStop's wrongful conduct, Plaintiff and Class members were injured in that they would not have allowed their sensitive Card Information—the value of which Plaintiff and Class members no long have control—to be provided to GameStop if they had been told or knew that GameStop failed to maintain sufficient security to keep such data from being hacked and taken by others.

149. GameStop's unfair and/or deceptive conduct proximately caused Plaintiff's and Class members' injuries because, had GameStop maintained customer Card Information with adequate security, Plaintiff and the Class members would not have lost it.

150. As a direct and proximate result of GameStop's conduct, Plaintiff and Class Members have suffered harm, including but not limited to 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 at GameStop that Plaintiff and Class members would have never made had they known of GameStop's careless approach to cybersecurity; 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; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information entitling them to damages in an amount to be proven at trial.

151. Defendants acted with willful and conscious disregard of the rights of others, subjecting Plaintiff and Class members to unjust hardship as a result such that an award of punitive damages is appropriate.

152. Plaintiff and the Class seek actual damages, compensatory, punitive damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the NCUDTPA. Plaintiff, individually and on behalf of the Class, seeks treble damages pursuant to N.C. GEN. STAT. § 75-16 and an award of reasonable attorneys' fees pursuant to N.C. GEN. STAT. § 75-16.1.

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)(3), 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, 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 customers' 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: September 29, 2017

Respectfully submitted,

/s/ Robert J. Kriner, Jr.

Robert J. Kriner, Jr. (Bar No. 2546)
Vera G. Belger (Bar No. 5676)
CHIMICLES & TIKELLIS LLP
222 Delaware Ave, Suite 1100
Wilmington, DE 19801
(302) 656-2500
rjk@chimicles.com
vgb@chimicles.com

Benjamin F. Johns
Andrew W. Ferich
Jessica L. Titler
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
awf@chimicles.com
jlt@chimicles.com

Cornelius P. Dukelow
Oklahoma Bar No. 19086
Abington Cole + Ellery
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com
www.abingtonlaw.com

Counsel for Plaintiffs and the Putative Class

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 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, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Crystal Bray and Samuel Cook

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Chimicles & Tikellis LLP, 222 Delaware Avenue, #1100, P.O. Box 1035 Wilmington, DE 19801; 302-656-2500

DEFENDANTS
Gamestop Corporation

County of Residence of First Listed Defendant New Castle County, DE
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

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)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*
Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	SOCIAL SECURITY	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	☐ 861 HIA (1395ff)	☐ 480 Consumer Credit
☐ 190 Other Contract	☒ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
☐ 196 Franchise				☐ 864 SSID Title XVI	☐ 890 Other Statutory Actions
				☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION		☐ 893 Environmental Matters
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	Habeas Corpus:	☐ 462 Naturalization Application	FEDERAL TAX SUITS	☐ 895 Freedom of Information Act
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 465 Other Immigration Actions	☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 896 Arbitration
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence		☐ 871 IRS—Third Party 26 USC 7609	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General			☐ 950 Constitutionality of State Statutes
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	Other:			
	☐ 448 Education	☐ 540 Mandamus & Other			
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

V. 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)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
Class Action Fairness Act 28 U.S.C. Section 1332(d)(2)
Brief description of cause:
Consumer Data Breach

VII. REQUESTED IN COMPLAINT:
☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.
DEMAND $
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*:
JUDGE _____ DOCKET NUMBER _____

DATE 9/29/2017
SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____