UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DARRELL KEMP, and BRADLEY COOPER, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

BONOBOS, INC.,

Defendant.

Case No. 1:21-cv-854

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Darrell Kemp and Bradley Cooper ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against Defendant Bonobos, Inc. ("Defendant" or "Bonobos"):

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant Bonobos for its failure to exercise reasonable care in securing and safeguarding its customers' personal identifying and financial information, including customers' addresses, phone numbers, partial credit card numbers, order information, and password histories (hereinafter, "Private Information").

2. Defendant Bonobos began as an upscale online men's clothing store, which later expanded to approximately sixty physical locations. In 2017, Walmart purchased Bonobos for $300 million to offer Bonobos' clothing on Walmart's Jet.com website.

3. To make purchases through Bonobos, customers must enter their name, address,

credit card information, and other personal details.

4. In January of 2021, a threat actor[1] known as ShinyHunters, who is notorious for hacking online services and selling stolen databases, posted Bonobos' private database to a hacker forum. The leaked database included a "70 GB SQL file" containing various internal tables used by the Bonobos website. The database reportedly included customers' addresses, phone numbers, partial credit card numbers (including the last four digits), order information, and password histories (the "Data Breach").[2]

5. On information and belief, the threat actor also turned the cracked passwords into a list used in credential stuffing attacks, which involves utilizing the log in information using the stolen credentials to access other websites.[3]

6. After being contacted by industry specialists, Bonobos claimed that the threat actors did not gain access to internal systems, but rather, to a backup file hosted in an external cloud environment. According to news reports, Bonobos stated:

> Protecting our customers' data is something we take very seriously. We're investigating this matter further and, so far, have found no evidence of unauthorized parties gaining access to Bonobos' internal system. What we have discovered is an unauthorized third party was able to view a backup file hosted in an external cloud environment. We contacted the host provider to resolve this issue as soon as we became aware of it. …
>
> Also, we have taken additional precautionary steps, including turning off access points, invalidating account passwords and requiring password resets, to further secure customer accounts. We're emailing customers to notify them that their contact information and encrypted passwords may have been viewed by an

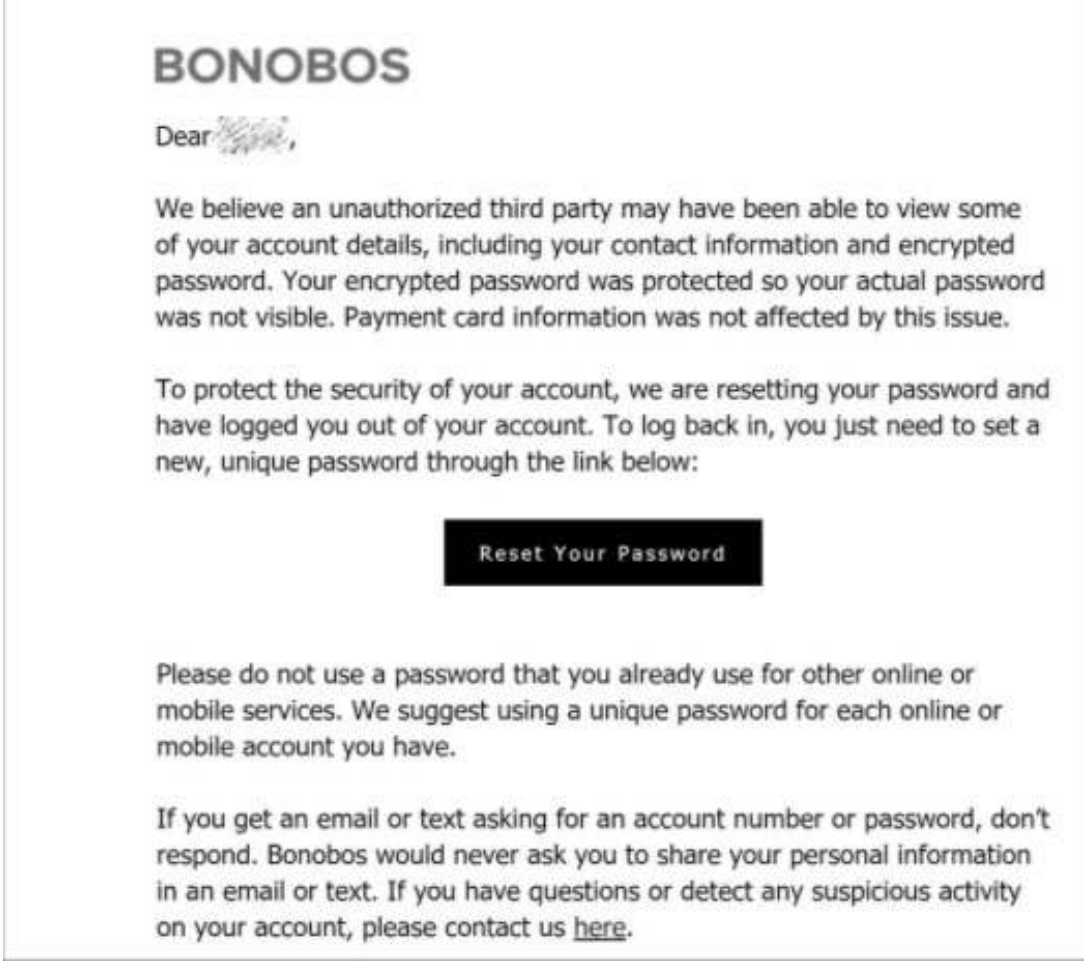
[1] A "threat actor," also called a malicious actor or bad actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organization's security. https://whatis.techtarget.com/definition/threat-actor (last accessed January 29, 2021).

[2] "Bonobos clothing store suffers a data breach, hacker leaks 70GB database," BleepingComputer, https://www.bleepingcomputer.com/news/security/bonobos-clothing-store-suffers-a-data-breach-hacker-leaks-70gb-database/ (last accessed January 29, 2021).

[3] Credential stuffing is the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force attach category: large numbers of spilled credentials are automatically entered into the websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes. *See Credential Stuffing*, https://owasp.org/www-community/attacks/Credential_stuffing (last accessed January 29, 2021).

unauthorized third party. Payment information was not affected by this issue.[4]

7. On or about January 24, 2021, Bonobos began emailing breach notifications to affected customers, with the following email message:



BONOBOS

Dear [redacted],

We believe an unauthorized third party may have been able to view some of your account details, including your contact information and encrypted password. Your encrypted password was protected so your actual password was not visible. Payment card information was not affected by this issue.

To protect the security of your account, we are resetting your password and have logged you out of your account. To log back in, you just need to set a new, unique password through the link below:

Reset Your Password

Please do not use a password that you already use for other online or mobile services. We suggest using a unique password for each online or mobile account you have.

If you get an email or text asking for an account number or password, don't respond. Bonobos would never ask you to share your personal information in an email or text. If you have questions or detect any suspicious activity on your account, please contact us here.

8. On information and belief, Plaintiffs' and Class members' Private Information was stolen by threat actors. Plaintiffs' and Class members' Private Information may be used for criminal purposes, such as identity theft and fraudulent purchases, and may be sold by the threat actors responsible for the Data Breach to other criminals on the dark web.

9. Defendant Bonobos' inadequate security failures enabled the threat actors to execute the Data Breach and steal Plaintiffs' and Class members' Private Information. The Data

[4] "Bonobos Suffers Huge Data Breach," BleepingComputer, https://risnews.com/bonobos-suffers-huge-data-breach (last accessed January 29, 2021).

Breach was caused and enabled by Defendant's violation of its obligations to abide by best practices and industry standards concerning the security of payment systems. Bonobos failed to properly comply with security standards that could have prevented or mitigated the Data Breach that occurred and allowed its customers' Private Information to be compromised.

10. Defendant Bonobos' failures put Plaintiffs' and Class members' financial information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiffs and Class members associated with time and money spent and the loss of productivity as a result of taking time and incurring costs to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach.

11. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class, assert claims for negligence, negligence *per se*, unjust enrichment, and violations of the New York consumer protection laws, and seek injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

12. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member (Plaintiff Kemp) is a citizen of a state that is diverse from Defendant's citizenship (New York), and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

13. The Court has personal jurisdiction over Defendant because Defendant maintains its headquarters in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York. Further, Defendant's officers direct, control and coordinate Bonobos' actions from New York.

14. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District

pursuant to 28 U.S.C. § 1391(c)(2).

III. PARTIES

Plaintiffs

15. Plaintiff Darrell Kemp is a citizen and resident of the State of Ohio, residing at 1580 Lincoln Road, Columbus, Ohio 43212.

16. Plaintiff Bradley Cooper is a citizen and resident of the State of New York, residing at 165 Sterling Road, Harrison, NY 10528.

17. Plaintiffs Kemp and Cooper each received a data breach notice from Bonobos regarding the Data Breach.

18. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their Private Information, a form of intangible property that they entrusted to Defendant for the purpose of making online purchases, which Private Information was compromised as a result of the Data Breach. Additionally, Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud and identity theft and misuse posed by their Private Information being placed in the hands of criminals. In addition, Plaintiffs suffered actual damages because they spent many hours of their time that they will never get back, addressing the data breach.

19. Upon information and belief, Plaintiffs' Private Information has been made available to unauthorized third parties, including through the dark web, as a result of the Data Breach.

20. Plaintiffs have been and will be forced to take a number of time-consuming and burdensome measures as a result of the Data Breach, all of which afford them actual damages because they could and should have been using this time to work and earn a living.

21. Plaintiffs and the other Class members are also at risk of imminent and impending

injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Private Information being stolen by criminals in the Data Breach and, including, but not limited to, the extent that Plaintiffs and other Class members still have the payment cards they used to make purchases on websites operated by Defendant.

22. Plaintiffs and the other Class members have a continuing interest in ensuring that their Private Information is protected and safeguarded from future breaches.

23. The injuries suffered by Plaintiffs and Class members as a direct result of the Data Breach include one or more of the following:

a. unauthorized use of their Private Information;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Private Information;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiffs and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. damages to and diminution in value of their Private Information entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

h. the loss of Plaintiffs' and Class members' privacy.

Defendant

24. Defendant Bonobos, Inc. is a Delaware corporation with its principal place of business in New York, New York that operates an online men's clothing store serving customers throughout the United States, as well as approximately sixty physical locations.

25. Defendant Bonobos makes sizeable profits at the expense of its loyal customers; however, Bonobos betrayed the trust of its customers by willfully putting at risk of attack by cybercriminals their Private Information. Bonobos chose to maintain inadequate information technology systems, exposing its customers' Private Information, including highly sensitive personal and financial information, to cyberattack. Through this lawsuit, the numerous affected consumers who entrusted their Private Information to Bonobos have a voice in Plaintiffs Kemp and Cooper.

IV. FACTUAL BACKGROUND

The Data Breach

26. On or around January 22, 2021, Bonobos disclosed a data breach of its systems that impacted seven (7) million customers (defined herein as the "Data Breach"). The Data Breach included customers' email addresses, phone numbers, last four digits of credit card account numbers, account order information, and encrypted passwords.

27. Bonobos described the breach as follows:

> What we have discovered is an unauthorized third party was able to view a backup file hosted in an external cloud environment…. We contacted the host provider to resolve this issue as soon as we became aware of it. Also, we have taken additional precautionary steps, including turning off access points, invalidating account passwords and requiring password resets, to further secure customer accounts. We're emailing customers to notify them that their contact information and encrypted passwords may have been viewed by an unauthorized third party. Payment information was not affected by this issue.[5]

[5] "Bonobos Suffers Huge Data Breach," BleepingComputer, https://risnews.com/bonobos-suffers-huge-data-breach (last accessed January 29, 2021).

28. On or about January 24, 2021, Bonobos sent emails to affected customers, including Plaintiffs, regarding the Data Breach.

Defendant's Data Security Standards were Inadequate

29. Defendant was on notice of the very real risks of security breaches like the Data Breach. Security breaches like the Data Breach have been frequent and garnered significant media attention over the last decade, with significant data breaches dating back to 2005. The Privacy Rights Clearinghouse, a nonprofit organization which focuses on strengthening privacy protections, has recorded over 9,000 data-related security breaches in the U.S. since 2005, including numerous instances of hacking.[6] Any e-commerce provider – indeed, any business which collects Private Information – is well aware of the risk of security breaches and the need to ensure a robust system of safeguarding against security breaches.

30. Plaintiffs and other Class members relied on Defendant to have implemented and maintained systems that would keep their Private Information safe. Defendant had a duty to keep its customers' Private Information safe. Defendant failed to comply with this duty.

Defendant Failed to Comply with Industry Standards

31. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[7]

32. In 2016, the FTC updated its publication, *Protecting Personal Information: A*

[6] *Data Breaches*, Privacy Rights Clearinghouse, https://privacyrights.org/data-breaches (last visited January 29, 2021).
[7] *Start With Security*, Federal Trade Commission, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited January 29, 2021).

Guide for Business, which establishes guidelines for fundamental data security principles and practices for business.[8] The guidelines note 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; keep software updated; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting 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.

33. The FTC recommends that businesses limit who can access sensitive data; require complex passwords to be used on networks; use industry-tested methods to ensure security and avoid hacking; monitor for suspicious activity on the network; ensure coding in software used by the business is secure; test systems for common security vulnerabilities and verify that third-party service providers have implemented reasonable security measures.[9]

34. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

35. In addition, Defendant does not claim that it complies with the Payment Card

[8] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited January 29, 2021).

[9] Federal Trade Commission, *Start With Security*, *supra* note 11.

Industry Data Security Standard (PCI DSS).[10] The PCI DSS, formulated by the PCI Security Standards Council, sets out measures that should be taken to ensure data security in relation to online financial transactions. The PCI DSS is designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

36. The PCI DSS was developed to encourage cardholder data security by setting out minimum requirements for businesses to follow. PCI DSS compliance includes, at a minimum, developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks by using regularly updated anti-virus software.[11]

37. Despite Defendant's awareness of its data security obligations and its promises to customers that their personal data would be secured and protected, Defendant's treatment of Private Information entrusted to it by its customers fell far short of satisfying Defendant's legal duties and obligations, and included violations of the PCI DSS. Defendant failed to ensure that access to its data systems was reasonably safeguarded, failed to follow industry standards for the protection of Private Information and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

38. As a result of Defendant's failure to adhere to industry and government standards for the security of card data, Private Information of Defendant's customers, including Plaintiffs and Class members, was compromised.

Security Breaches Lead to Identity Theft

39. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 26 million people were victims of one or more incidents of identity theft in 2016.[12]

[10] PCI DSS, PCI Security Standards Council, *DocumentLibrary*, https://www.pcisecuritystandards.org/document_library (last accessed January 29, 2021).
[11] *Id*.
[12] *See* DOJ, *Victims of Identity Theft, 2016*, at 1 (Jan. 2019), https://www.bjs.gov/content/pub/pdf/vit16.pdf (last accessed

Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[13] There were 16.7 million fraud incidents in 2017, 14.4 million fraud incidents in 2018 and 13 million fraud incidents in 2019.[14] While the number of fraud incidents fell between 2018 and 2019, the total amount of money lost to fraud increased, with $16.9 billion in fraud losses in 2019.[15] At least one commentator has determined that 77.3 percent of identity theft victims report emotional distress.[16]

40. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[17]

41. Private Information—which includes Plaintiffs' and Class members' names and their payment card information that were stolen in the Data Breach—is a valuable commodity to identity thieves. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information disclosed by customers on the websites Defendant operates is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

42. Stolen Private Information is a valuable commodity. A "cyber black-market" on the dark web exists, in which criminals openly post stolen payment card numbers, social security

---

Jan. 29, 2021).

[13] *Id*.

[14] See *Identity theft facts & statistics: 2019-2020* (Nov. 13, 2020), https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/ (last accessed Jan. 29, 2021).

[15] *Id*.

[16] See Identity Theft Center Resource Center, *The Non-Economic Impacts of Identity Theft* (2018), https://www.idtheftcenter.org/wp-content/uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf (last accessed Jan. 29, 2021).

[17] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id*.

numbers, and other personal information on a number of underground Internet websites. Identity thieves use stolen Private Information to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards. Stolen Private Information may be traded on the dark web for years.

43. The growing sophistication of hackers and threat actors to commit identity theft and fraud are of serious concern and directly implicated in the Data Breach. Hackers and threat actors are able to gain access to a wide variety of an individual's personal accounts through minimal information.[18] For example, "a billing address and the last four digits of a credit card number are the only two pieces of information anyone needs to get into your iCloud account."[19] From there, "hackers were able to […] take over all of [an individual's] digital devices – and data."[20] Further, hackers have the capability to generate a CVV code "starting with no details at all other than the first six digits" of a payment card, thereby enabling "hackers [to] obtain the three essential pieces of information to make an online purchase within as little as six seconds."[21]

44. The National Institute of Standards and Technology categorizes the combination of names and credit card numbers as sensitive and warranting a higher impact level based on the potential harm when used in contexts other than their intended use.[22] Private Information that is "linked" or "linkable" is also more sensitive. Linked information is information about or related to an individual that is logically associated with other information about the individual. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. An example of linking information

---

[18] Mat Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking*, (August 6, 2012) https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ (last visited January 29, 2021).
[19] *Id.*
[20] *Id.*
[21] Newcastle University, *Six Seconds to Hack a Credit Card* (Dec. 2, 2016) https://www.ncl.ac.uk/press/articles/archive/2016/12/cyberattack/ (last visited January 29, 2021).
[22] Erika McCallister, *et al.*, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology Special Publication 800-122, 3-3, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904990 (last visited January 29, 2021).

the NIST report cites is a Massachusetts Institute of Technology study showing that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth.

45. Private Information is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

The Monetary Value of Privacy Protections and Private Information

46. The fact that Plaintiffs' and Class members' Private Information was stolen, likely in order to be sold on the dark web and/or used for fraudulent transactions, demonstrates the monetary value of the Private Information.

47. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[23]

48. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[24]

49. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

---

[23] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace- merging-and-exchanging-consumer-data/transcript.pdf (last visited Jan. 29, 2021).

[24] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Jan. 29, 2021).

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[25]

50. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[26] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

51. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[27]

52. The value of Plaintiffs' and Class members' Private Information on the black market is substantial, ranging from $1.50 to $90 per card number.[28]

53. Despite being aware of the value criminals attach to such Private Information, Defendant failed to ensure its customers were protected from the theft of their Private Information.

54. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

---

[25] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited January 29, 2020).

[26] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Jan. 29, 2021).

[27] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Jan. 29, 2021), at 6.

[28] Leapfrog, *The Cyber Black Market: What's Your Bank Login Worth* (Mar. 1, 2011), https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/ (last visited Jan. 29, 2021).

55. Had Defendant remedied the deficiencies in its e-Commerce systems, adequately monitored its e-commerce systems for malicious codes, followed PCI DSS guidelines and, in general, taken reasonable care to prevent and detect security breaches, the Data Breach would have been prevented.

56. Given these facts, any company that transacts business with consumers – who expect their Private Information to be properly safeguarded - and then compromises the privacy of consumers' Private Information has thus deprived consumers of the full monetary value of their transaction with the company.

Damages Sustained by Plaintiffs and Class Members

57. A portion of the services purchased from Defendant by Plaintiffs and the other Class members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of Private Information, including their credit and debit card information. The cost to Defendant of collecting and safeguarding Private Information is built into the price of all its services. Because Plaintiffs and the other Class members were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the other Class members incurred actual monetary damages in that they overpaid for the purchases they made through websites operated by Defendant.

58. Plaintiffs and the other members of the Class have suffered additional injury and damages, including, but not limited to one or more of the following:

a. unauthorized use of their Private Information;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Private Information;

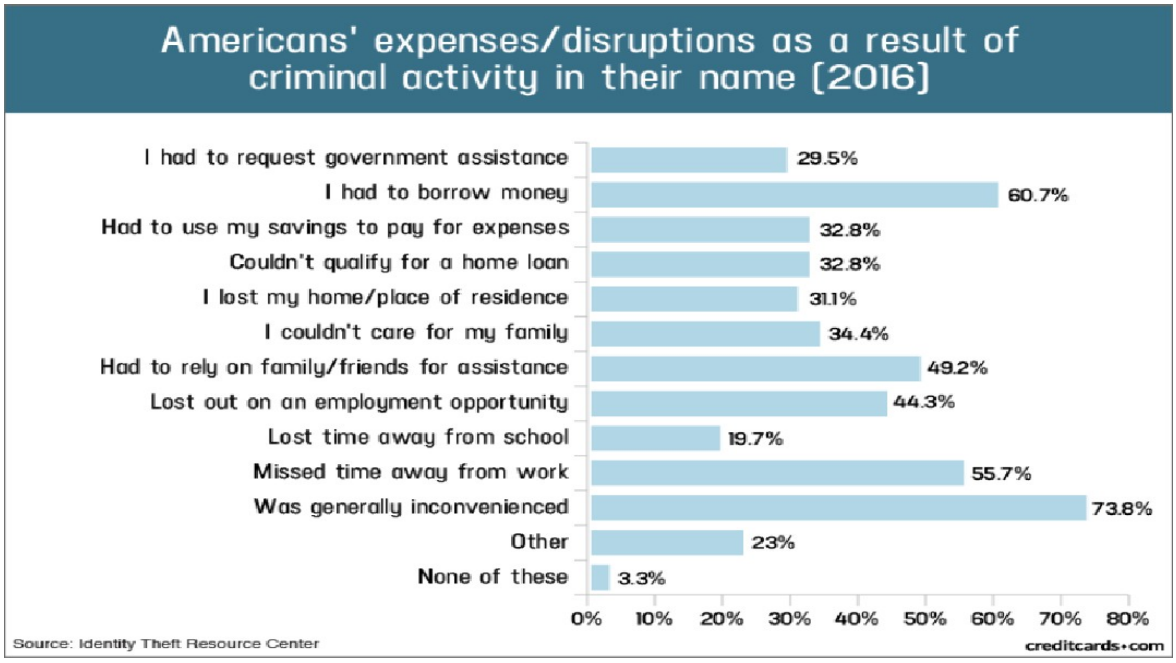
e. time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiffs and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. damages to and diminution in value of their Private Information entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

h. the loss of Plaintiffs' and Class members' privacy.

59. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal information:[29]



[29] Jason Steele, Credit Card and ID Theft Statistics (Oct. 24, 2017) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited January 29, 2021).

V. CLASS ACTION ALLEGATIONS

60. Plaintiffs bring all counts, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a nationwide Class defined as:

> **All residents of the United States of America whose Private Information was compromised in the Data Breach.**

61. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

62. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

63. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number in the tens if not hundreds of thousands.

64. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class members' Private Information;

b. Whether Defendant properly implemented its purported security measures to protect Plaintiffs' and Class members' Private Information from unauthorized

capture, dissemination, and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

d. Whether Defendant disclosed Plaintiffs' and Class members' Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

e. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Private Information;

f. Whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and Class members' Private Information; and

g. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

65. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other Class members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

66. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

67. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

68. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23(b)(2).

69. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

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

70. Plaintiffs, individually and on behalf of the Class, repeat and re-allege the

allegations contained in paragraphs 1 through 69 as though fully set forth herein.

71. Upon accepting and storing Plaintiffs' and Class members' Private Information in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was confidential and should be protected as private and confidential.

72. Defendant owed a duty of care not to subject Plaintiffs' and Class members' Private Information to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

73. Defendant owed numerous duties to Plaintiffs and Class members, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

74. Defendant also breached its duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was, and is, entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' Private Information, misuse the

Private Information and intentionally disclose it to others without consent.

75. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information, the vulnerabilities of its data collection and/or storage systems, and the importance of adequate security.

76. Defendant knew, or should have known, that its data collection and/or storage systems and networks did not adequately safeguard Plaintiffs' and Class members' Private Information.

77. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

78. Because Defendant knew that a breach of its systems would damage an untold number of its customers, including Plaintiffs and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

79. Defendant had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems, and the Private Information it stored on them, from attack.

80. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Upon information and belief, Defendant's misconduct included failing to: (1) secure its data collection and/or storage systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

81. Defendant also had independent duties under state and federal laws that required it to reasonably safeguard Plaintiffs' and Class members' Private Information and promptly notify them about the Data Breach.

82. Defendant breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information;
b. by creating a foreseeable risk of harm through the misconduct previously described;
c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' Private Information both before and after learning of the Data Breach;
d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and
e. by failing to timely disclose that Plaintiffs' and Class members' Private Information had been improperly acquired or accessed.

83. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendant's possession or control.

84. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Private Information to Plaintiffs and the Class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information. Defendant failed to do so, only disclosing

the Data Breach almost a month after it was detected.

85. Defendant further breached its statutory duties designed to protect the public from harms caused by data breaches, including but not limited to duties to use reasonable measures to protect Private Information imposed by Section 5 of the Federal Trade Commission Act (the "FTCA").

86. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and their failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendant's possession or control.

87. Upon information and belief, Defendant improperly and inadequately safeguarded Plaintiffs' and Class members' Private Information in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect Plaintiffs' and Class members' sensitive Private Information, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the Private Information.

88. Upon information and belief, neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

89. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered Plaintiffs and Class members have suffered and will suffer damages and injury, including but not limited to:

a. unauthorized use of their Private Information;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Private Information;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiffs and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. damages to and diminution in value of their Private Information entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

h. the loss of Plaintiffs' and Class members' privacy.

90. As a direct and proximate cause of Defendant's negligence, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

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

91. Plaintiffs, individually and on behalf of the Class, repeat and re-allege the allegations contained in paragraphs 1 through 69 as though fully set forth herein.

92. Section 5 of the FTCA bars unfair and deceptive acts and practices "in or affecting commerce," which the FTC has interpreted and enforced as including action against organizations that have violated consumers' privacy rights and/or misled consumers through a failure to maintain appropriate security for sensitive information, such as the Private Information of Plaintiffs and Class members. The FTC guidance discussed above also serves to further the Defendant's duty to Plaintiffs and Class members.

93. Defendant violated Section 5 of the FTCA in its failure to implement reasonable safeguards to protect the Private Information of Plaintiffs and Class members and in its abandonment of industry standards regarding the protection of consumers' Private Information. Defendant's violation of Section 5 of the FTCA is all the more unreasonable in light of the vast size of Defendant's consumer base, as well as the particularly sensitive nature of Plaintiffs' and Class members' Private Information that was collected and stored.

94. Defendant's violation of Section 5 of the FTCA is negligence *per se*.

95. Plaintiffs and Class members are within the class of persons that the FTCA intends to protect.

96. The harm sustained by Plaintiffs and Class members as a result of the Data Breach is the type of harm that the FTCA was intended to safeguard the public against. The FTC has taken enforcement action against organizations failing to implement reasonable and proper measures to protect consumers' sensitive data, as these acts constitute unfair and deceptive practices. These harms are the same as those suffered by Plaintiffs and Class members in this action.

97. As a direct and proximate cause of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to:

a. unauthorized use of their Private Information;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Private Information;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiffs and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. damages to and diminution in value of their Private Information entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

h. the loss of Plaintiffs' and Class members' privacy.

98. As a direct and proximate cause of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Violations of New York Consumer Law for Deceptive Acts and Practices
N.Y. Gen. Bus. Law § 349
(On Behalf of Plaintiffs and the Class)

99. Plaintiffs, individually and on behalf of the Class, repeat and re-allege the allegations contained in paragraphs 1 through 69 as though fully set forth herein.

100. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

101. The law of the State of New York applies to all customer disputes with respect to customer purchases from Defendant's e-commerce websites.

102. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred in part within New York State.

103. Defendant stored Plaintiffs' and the Class members' Private Information in Defendant's electronic and consumer information databases. Defendant knew or should have known that it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the Class members' Private Information secure and prevented the loss or misuse of Plaintiffs' and the Class members' Private Information. Defendant did not disclose to Plaintiffs and the Class members that its data systems were not secure.

104. Plaintiffs and the Class members never would have provided their sensitive and personal Private Information if they had been told or knew that Defendant failed to maintain sufficient security to keep such Private Information from being hacked and taken by others, and that Defendant failed to maintain the information in a properly encrypted form.

105. Defendant violated the NYGBL §349 by failing to properly represent, both by affirmative conduct and by omission, the safety of Defendant's many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and the Class members' Private Information.

106. Defendant also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or adequately follow industry standards for data security, and by failing to immediately notify Plaintiffs and the Class members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the extent of damages caused by the Data Breach.

107. Defendant's practices, acts, policies and course of conduct violate NYGBL § 349 in that:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiffs and the Class members at the time they provided such Private Information that Defendant did not have sufficient security or mechanisms to protect Private Information;

b. Defendant failed to give timely warnings and notices regarding the defects and problems with its system(s) of security that it maintained to protect Plaintiffs' and the Class members' Private Information.

108. Plaintiffs and Class members were entitled to assume, and did assume, Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any time that Plaintiffs' and the Class members' Private Information was vulnerable to hackers because Defendant's data security measures were inadequate, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

109. The aforementioned conduct constitutes an unconscionable commercial practice in

that Defendant has, by the use of false statements and/or material omissions, failed to properly represent and/or concealed the defective security system it maintained and failed to reveal the Data Breach timely and adequately.

110. Members of the public were deceived by and relied upon Defendant's affirmative misrepresentations and failures to disclose.

111. Such acts by Defendant are and which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendant. Said acts and practices are material. The requests for and use of such Private Information in New York through such means occurring in New York were consumer-oriented acts and thereby fall under the New York consumer protection statute, NYGBL § 349.

112. Defendant's wrongful conduct caused Plaintiffs and the Class members to suffer a consumer-related injury by causing them to incur actual and future loss of time and expense to protect from misuse of the Private Information materials by third parties and placing the Plaintiffs and the Class members at serious risk for monetary damages.

113. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

114. In addition to or in lieu of actual damages, because of the injury, Plaintiffs and the Class members seek statutory damages for each injury and violation which has occurred.

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

115. Plaintiffs, individually and on behalf of the Class, repeat and re-allege the allegations contained in paragraphs 1 through 69 as though fully set forth herein.

116. Plaintiffs and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their

payment information. In exchange, Plaintiffs and Class members should have received from Defendant the goods and services that were the subject of the transaction with protection of their Private Information with adequate data security.

117. Defendant knew that Plaintiffs and Class members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendant profited from Plaintiffs' purchases and used Plaintiffs' and Class members' Private Information for business purposes.

118. Defendant failed to secure Plaintiffs' and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members' Private Information provided.

119. Defendant acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

120. If Plaintiffs and Class members knew that Defendant would not secure their Private Information using adequate security, they would not have made purchases on Defendant's website.

121. Plaintiffs and Class members have no adequate remedy at law.

122. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

123. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class members overpaid.

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their and the Class' favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Class Counsel as requested in Plaintiffs' expected motion for class certification;

B. Ordering Defendant to pay actual/statutory damages as appropriate to Plaintiffs and the other members of the Class;

C. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

D. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiffs and their counsel;

E. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Date: January 29, 2021.

Respectfully submitted,

/s/ Lori G. Feldman
Lori G. Feldman (LF-3478)
GEORGE GESTEN MCDONALD PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Phone: (917) 983-9321
Fax: (888) 421-4173
Email: LFeldman@4-Justice.com
E-Service: eService@4-Justice.com

David J. George (*pro hac vice* forthcoming)
Brittany L. Brown (*pro hac vice* forthcoming)
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Phone: (561) 232-6002
Fax: (888) 421-4173
Email: DGeorge@4-Justice.com
BBrown@4-Justice.com
E-Service: eService@4-Justice.com

Terence R. Coates (*pro hac vice* forthcoming)
Justin C. Walker (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
Email: tcoates@msdlegal.com
jwalker@msdlegal.com

Attorneys for Plaintiffs