**IN THE UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF ILLINOIS**

| | |
|---|---|
| DELILAH PARKER and KELVIN HOLMES, Individually and on Behalf of All Others Similarly Situated,<br><br>Plaintiffs,<br><br>v.<br><br>CLAIRE'S STORES, INC.; CLAIRE'S BOUTIQUES, INC. and CBI DISTRIBUTING CORP.,<br><br>Defendants. | Case No.:<br><br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Plaintiffs Delilah Parker and Kelvin Holmes (collectively, "Plaintiffs") bring this Class Action Complaint against Claire's Stores, Inc., Claire's Boutiques, Inc., and CBI Distributing Corp. (collectively, "Claire's" or "Defendants") on behalf of themselves and all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

## NATURE OF THE ACTION

1. Claire's specializes in selling low-price jewelry and accessories to young women and girls. Defendants operate internationally through their retail stores under two brand names, Claire's® and Icing®. Defendants also sell their products online through their popular websites. For online sales, Defendants use ecommerce platforms supported by salesforce.com, inc. to take customers' personal and payment information.

2. On or about July 7, 2020, Claire's began notifying customers and state Attorneys General about a widespread data breach that occurred from at least April 7, 2020 through June 12, 2020 (the "Data Breach"). Hackers not only "scraped" many of Defendants' customers' full names from the website by infecting it with a malicious code, hackers also stole customers'

addresses, email addresses, telephone numbers, payment card numbers, CVV security codes, and payment card expiration dates. The hackers got everything they needed to illegally use Claire's customers' payment cards to make fraudulent purchases, and to steal customers' identities.

3. All of this personally identifiable information ("PII") was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to their failure to prevent the Data Breach, Defendants failed to detect and report the breach for months.

4. Defendants had no idea the breach was happening. Claire's investigated their ecommerce website only after they were contacted by a third-party on June 11, 2020, who determined that the ecommerce platforms on Claires.com and Icing.com had been hacked.[1] According to Claire's, Defendants discovered that the "added code was capable of obtaining information entered by customers during the checkout process and sending it out of the Claire's system."

5. Defendants hired an outside security firm to investigate. The security firm identified the specific transactions involved and determined that purchases made in Defendants' retail locations were not involved. The firm also discovered that that the malicious code was first inserted into the ecommerce platforms on April 7, 2020. Defendants did not begin notifying affected customers and states' Attorneys General until three months later, on or about July 7, 2020.

6. The stolen PII has great value to hackers due to its thoroughness and the numbers involved: It is likely that this breach stole the full payment card information for tens of thousands of customers. For example, the Washington State Attorney General reports that 1,166 Washingtonians were affected, and the Indiana Attorney General reports 1,257.

[1] *See, e.g.*, Exhibit 1, Claire's *Notice of Data Breach to the Washington Attorney General*, July 8, 2020, archived by the Washington Attorney General, *available at*: https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/Claire%27sStoresInc.2020-07-08.pdf (Claire's *Notice of Data Breach*, addressed to affected customers, is included at pages 3-7) (last accessed on Aug. 25, 2020).

7. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect its users' PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor Defendants' websites and ecommerce platforms for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

8. Plaintiffs and similarly situated customers ("Class members") have suffered injury as a result of Defendants' conduct. These injuries may include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) deprivation of rights they possess under the Illinois Consumer Fraud and Deceptive Trade Practices Act (815 ILCS § 505/1, *et seq*.) and the Illinois Personal Information Protection Act (815 ILCS 530/1, *et seq*.); (v) deprivation of rights they possess under the Tennessee Consumer Protection Act, Tenn. Code. Ann. §§ 47-18-101, *et seq*.; (vi) the continued and certainly an increased risk to their PII, which (a) may remain available on the dark web for individuals to access and abuse, and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

## PARTIES

9. Plaintiff Delilah Parker is a citizen of Tennessee residing in Davidson County. Ms. Parker purchased items from Claire's website on or about May 24, 2020. She received Claire's *Notice of Data Breach*, dated July 7, 2020, on or about that date, which specially identified her debit card as the payment card exposed by the Data Breach.

10. Plaintiff Kelvin Holmes is a citizen of Georgia residing in Cedartown, Georgia. Mr. Holmes purchased items from Claire's website on or about May 25, 2020. He received Claire's *Notice of Data Breach*, dated July 7, 2020, on or about that date, which specially identified his debit card as the payment card exposed by the Data Breach.

11. Defendant Claire's Stores, Inc. is a Florida corporation with its principal place of business in Hoffman Estates, Illinois. During the class period, Claire's operated across the United States through its websites and sold jewelry and other clothing accessories at its retail locations throughout the nation and at least 28 other countries.

12. Defendant Claire's Boutiques, Inc. is a Michigan corporation with its principal place of business in Hoffman Estates, Illinois. Upon information and belief, Claire's Boutiques, Inc. is a wholly owned subsidiary of Claire's Stores, Inc. that operates the Claire's ecommerce websites. Prior to September 4, 2020, Claire's Boutiques, Inc. was a Colorado corporation.

13. Defendant CBI Distributing Corp. is a Delaware corporation with its principal place of business in Hoffman Estates, Illinois. Upon information and belief, CBI Distributing Corp. is a wholly owned subsidiary of Claire's Stores, Inc. that operates the Claire's ecommerce websites.

## JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants. Moreover, this Court has jurisdiction over this action under 28 U.S.C. § 1332(a)(1) because Plaintiff Parker is a Tennessee citizen, and Plaintiff Holmes is a Georgia resident, and therefore diverse from Defendants, which are not citizens of Tennessee or Georgia, but of other states.

15. This Court has personal jurisdiction over Defendants because Defendants have systematic and continuous contacts with the state through their websites and because their headquarters are located here.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendants reside within this judicial district and substantial part of

the events giving rise to the claims alleged herein occurred within this judicial district.

## FACTUAL ALLEGATIONS

### *Claire's Background*

17. Claire's is a popular jewelry chain for young girls and teens with almost 3,500 retail locations worldwide. Defendants also have a substantial online business through various websites, including claires.com and icing.com. In 2019, Defendants' global net sales for online purchases were reportedly $12.9 million.

18. Defendants ensure their customers that they are concerned about PII security: "We take data privacy very seriously and work super hard to protect your personal information."[2] *Super hard* is apparently not hard enough. Defendants also claim:

> SECURITY
> We believe in providing a safe and secure experience for all of our customers and the Site visitors. To that end we have implemented security measures to protect the information collected from you. All information you provide to us is stored on our secure servers and on the servers of cloud-based service providers. The computers and servers on which we store personal information are kept in a secure environment. **While we use encryption to protect sensitive information transmitted online, we also protect your information offline**. Payment transactions may be undertaken by third party service providers and will be encrypted using industry standard SSL technology. Where we have given you (or where you have chosen) a password which enables you to access your online account, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.
>
> We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it. Every employee accessing systems containing your personal information has a separate unique username and password. Access to your personal information is limited to those employees who require such access to perform their job duties. In addition, we train our employees about the importance of confidentiality and maintaining the privacy and security of your personal information. We commit to taking appropriate disciplinary measures to enforce our employees' privacy responsibilities [.] (emphasis added).[3]

[2] Claire's *Privacy Policy*, dated May 15, 2018, *available at*: https://www.claires.com/us/privacy-policy.html (last visited Aug. 25, 2020).

[3] *Id.*; *see also* Icing's *Privacy Policy*, which mirrors Claire's verbatim, *available at*: https://www.icing.com/us/privacy-policy.html (last visited Aug. 25, 2020).

19. Defendants do not claim that they abide by the PCI DSS (Payment Card Industry Data Security Standard) compliance, which is a requirement for businesses that store, process, or transmit payment card data.

20. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions. Businesses that fail to maintain PCI DSS compliance are subject to steep fines and penalties.

21. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: 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 using anti-virus software and updating it regularly.[4]

22. To purchase items on Defendants' websites, customers can either create an account or check out as a guest. Either choice requires, at a minimum, that the customer enter the following PII onto the website:

- Name;
- billing address;
- shipping address;
- email address;
- telephone number;
- name on the payment card;
- type of payment card;
- full payment card number;
- payment card expiration date; and
- security code or CVV code (card verification number).

23. When a customer purchases items on Defendants' websites, as a guest or through an account, they are not asked to acknowledge the "Privacy Policy," and they are not asked to

[4] PCI Security Standards Council, *available at*: https://www.pcisecuritystandards.org/ (last accessed Aug. 25, 2020).

read the "Terms of Use." Links to Claire's and Icing's "Privacy Policy" and "Terms of Use" are included on the extreme bottom right borders of the website pages in black, unremarkable font, with no indications of hyperlinks to the policies or terms. The "Privacy Policy" and "Terms of Use," however, do not appear at all on the mobile webpage unless the user clicks on the "About Us" link. Similarly, there are no links to the "Terms of Use" on the ecommerce platform where the purchase is finalized, only a terse statement in uniform font stating that the customer is "agreeing to our terms and conditions."

***The Data Breach***

24. Starting on or about July 7, 2020, Claire's mailed customers a *Notice of Data Breach*.[5] Claire's Executive Director of Communications and Operations, Marie Hodge, informed Claire's and Icing's affected customers that:

> What Happened?
> We recently began an investigation of our e-commerce websites, and on June 12, 2020 we identified and removed computer code that had been added to our site by an unauthorized person. The added code was capable of obtaining information entered by customers during the checkout process and sending that information out of our system. A security firm was engaged and we identified the specific transactions involved. We also reinforced the security of our site.
>
> Purchases made in our retail store locations were not involved. Findings from the investigation show the code was first added on April 7, 2020. There were several times from April 7 to June 12 when the added code was not present because of new code deployments. We are notifying you because you placed an order during a time the added code was present.
>
> What Information Was Involved?
> The information entered during the checkout process that could have been copied includes:
>
> - Contact information - first and last name, address, email address (only if you chose to edit your email on the checkout page), and phone number.
> - Payment card information - payment card number, expiration date, and card verification code for the payment card ending in [CARD NUMBER]. If you made more than one purchase between April 7 and June 12 and used more than one card, you can identify the other cards involved by looking at your email receipt or by calling us at the number below.

[5] Ex. 1 at 3-7.

- Other information - if you paid with a gift card or created a Claire's account during the checkout process, the added code could have copied the gift card number and PIN or the account password (but not email address).

25. Defendants' letter to the state Attorneys General provided more information about what occurred.

> Claire's began an investigation of its e-commerce websites after it was contacted by a security researcher the night of Thursday, June 11, 2020 who claimed to have determined that Claire's e-commerce site had been compromised. Claire's immediately took action to investigate the security researcher's claim and identified and removed unauthorized code in the code that operates its e-commerce site on Friday, June 12, 2020. The added code was capable of obtaining information entered by customers during the checkout process and sending it out of the Claire's system.[6]

26. Before the Data Breach, on or about March 21, 2020, an unidentified third-party anonymously registered the domain name "claires-assets.com."[7] Between April 25 and 30, 2020, malicious code was added to Claire's and Icing's ecommerce platforms. The code changed legitimate files on the ecommerce platforms, enabling the data exfiltration. As customers entered their payment information into the salesforce.com shopping cart, the malicious code essentially took a snapshot of the information, sent it to the claires-assets.com server, then deleted the image. Hacks like this typically end with the attackers selling the scraped data on the dark web.

27. Defendants admit that they did not detect the Data Breach. Claire's customers' information was scraped by hackers and available to other criminals and, on information and belief, may still be for sale to criminals on the dark web. Even though Defendants promised its customers that they "use encryption to protect sensitive information transmitted online,"[8] unauthorized individuals accessed Defendants' customers' unencrypted, unredacted information, including name, address, and payment card information, which includes payment card number,

---

[6] Exhibit 1 at 1.

[7] Zephyrnet.com, *Jewelry Chain Claire's Hit By eCommerce Mageware Attack* (06/17/2020) *available at*: https://zephyrnet.com/jewelry-chain-claires-hit-by-ecommerce-mageware-attack/ (last visited Aug. 25, 2020).

[8] Claire's *Privacy Policy*, dated May 15, 2018, at 10, *available at*: https://www.claires.com/us/privacy-policy.html (last visited Aug. 25, 2020).

CVV code, expiration date, and possibly more.

***Scraping and E-Skimming Breaches***

28. *Magecart* is a loose affiliation of hacker groups responsible for skimming payment card attacks on various companies, including British Airways and Ticketmaster.[9] Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart), and proceed to scrape credit card information to sell on the dark web.[10]

29. The hackers target what they refer to as the *fullz*–a term used by criminals to refer to stealing the full primary account number, card holder contact information, credit card number, CVC code, and expiration date. The *fullz* is exactly what Claire's admits the malware infecting its ecommerce platform scraped.

30. These cyber-attacks exploit weaknesses in the code of the ecommerce platform, without necessarily compromising the victim website's network or server.[11] These attacks often target third-party payment processors like Shopify, and, as is the case here, Salesforce.[12]

31. Magecart and these scraping breaches are not new: RiskIQ's earliest Magecart observation occurred on August 8th, 2010.[13] Thus, Defendants would have been made aware of this type of breach since that time, especially considering the surge of these types of breaches in the last few years.

32. Unfortunately, despite all of the publicly available knowledge of the continued compromises of PII in this manner, Defendants' approach to maintaining the privacy and

[9] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last accessed Aug. 25, 2020).
[10] *Id*.
[11] *What is Magecart and was it behind the Ticketmaster and BA hacks?*, Computerworld, Sep. 18, 2018, *available at*: https://www.idgconnect.com/idgconnect/news/1029449/magecart-ticketmaster-hacks (last accessed Aug. 27, 2020).
[12] *Id*.
[13] *Magecart: New Research Shows the State of a Growing Threat*, RiskIQ, Oct. 4, 2019, *available at*: https://www.riskiq.com/blog/external-threat-management/magecart-growing-threat/ (last accessed Aug. 25, 2020).

security of Plaintiffs' and Class members' PII was negligent, or, at the very least, Defendants did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect their customers' valuable PII.

***Value of Personally Identifiable Information***

33. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5-110 on the dark web; the *fullz* sold for $30 in 2017.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

34. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

35. Defendants were, or should have been, fully aware of the significant volume of daily credit and debit card transactions on its website – the malware infected Claire's ecommerce as its retail locations closed and customers could only get Claire's products from Defendants' websites – amounting to potentially hundreds of thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

---

[14] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Aug. 25, 2020).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Aug. 25, 2020).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Aug. 25, 2020).

***Plaintiff Parker's Experience***

36. Plaintiff Delilah Parker accessed Claire's website from her home on or about May 24, 2020 via her smartphone and purchased items for a total of $29.01, order number 8901806. The items were shipped to her by Claire's on or about May 28, 2020.

37. Ms. Parker made this purchase through the claires.com website as a guest. She entered her PII into Defendants' ecommerce payment platform, including her full name, billing and shipping addresses, debit card type and full number, CVV code, debit card expiration date and email address.

38. During this transaction, Ms. Parker was not asked or directed to "agree" to or even review Claire's "Privacy Policy," nor was she instructed to read the "Terms of Use."

39. Ms. Parker received the *Notice of Data Breach*, dated July 7, 2020, on or about that date. She did not receive the letter sent by Defendants to Attorneys General.

40. Beginning on or about August 17, 2020, unknown third-parties used Ms. Parker's debit card – the same payment card she used on Defendants' hacked ecommerce platform – to make unauthorized purchases in Washington, Georgia, and California via the internet. The purchases have totaled over $700 so far. The money was withdrawn from Ms. Parker's checking account on or about August 18, 2020, and although her bank confirmed the charges were unauthorized, the bank did not fully reimburse her for the losses until August 24, 2020.

41. As a result of the Data Breach notice and the subsequent theft of her funds, Ms. Parker spent time dealing with the consequences of the breach, which includes time spent confirming that she made a purchase using her debit card during the relevant period, reviewing the account compromised by the breach, contacting her bank, self-monitoring her accounts, exploring credit monitoring and identity theft insurance options, and signing up for the free credit monitoring service offered by Claire's.

42. Although Ms. Parker enrolled in the credit monitoring offered by Claire's in July 2020, the monitoring did not help prevent or notify her about the unauthorized use of her debit card in August 2020. In the *Notice of Data Breach,* Claire's did not advise affected customers to

change their payment card account numbers. Rather, Claire's stated that they already "notified the payment cards network so that they can inform the banks that issued the cards," and encouraged victims only "to closely review your payment card account statements for any unauthorized charges."[17]

43. Ms. Parker is not aware of any other data breaches that could have resulted in the theft of her debit card information. She is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

44. Ms. Parker stores any and all documents containing her PII in a safe and secure digital location, and destroys any documents she receives in the mail that contain any of her PII or that may contain any information that could otherwise be used to compromise her payment card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

45. Ms. Parker suffered actual injury and damages in losing aver $700 from her bank account and in paying money to, and purchasing products from, Defendants' website during the Data Breach—expenditures which she would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

46. Ms. Parker suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

47. Ms. Parker suffered lost money, time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of her privacy.

[17] Exhibit 1 at 3.

48. Ms. Parker has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

49. Ms. Parker has become paranoid and scared about this theft of her personal information, and has a continuing interest in ensuring that her PII, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

***Plaintiff Holmes' Experience***

50. Plaintiff Kelvin Holmes accessed Claire's website from his home on or about May 25, 2020 via his smartphone and purchased items for a total of $27.65, order number 8907419. The items were shipped to him by Claire's on or about May 25, 2020.

51. Mr. Holmes made this purchase through the claires.com website as a guest. He entered his PII into Defendants' ecommerce payment platform, including his full name, billing and shipping addresses, telephone number, debit card type and full number, CVV code, debit card expiration date and email address.

52. During this transaction, Mr. Holmes was not asked or directed to "agree" to or even review Claire's "Privacy Policy," nor was he instructed to read the "Terms of Use."

53. Mr. Holmes received the *Notice of Data Breach*, dated July 7, 2020, on or about that date. He did not receive the letter sent by Defendants to Attorneys General.

54. Subsequent to the Data Breach, Mr. Holmes began receiving a marked increase in the number of suspicious phishing emails containing fraudulent links. Reviewing these emails to determine their legitimacy has taken time that Mr. Holmes otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

55. As a result of the Data Breach notice and the subsequent suspicious emails, Mr. Holmes spent time dealing with the consequences of the breach, which includes time spent confirming that he made a purchase using his debit card during the relevant period, reviewing the account compromised by the breach, contacting his bank, self-monitoring his accounts, exploring credit monitoring and identity theft insurance options, and signing up for the free credit

monitoring service offered by Claire's.

56. Mr. Holmes is not aware of any other data breaches that could have resulted in the theft of his debit card information. He is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

57. Mr. Holmes stores any and all documents containing his PII in a safe and secure digital location, and destroys any documents he receives in the mail that contain any of his PII or that may contain any information that could otherwise be used to compromise his payment card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts, and periodically changes his passwords for added security.

58. Mr. Holmes suffered actual injury being forced to review phishing emails and in paying money to, and purchasing products from, Defendants' website during the Data Breach—expenditures which he would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

59. Mr. Holmes suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

60. Mr. Holmes suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of his privacy.

61. Mr. Holmes has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

62. Mr. Holmes has become scared and worried about this theft of his personal information, and has a continuing interest in ensuring that his PII, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

## CLASS ALLEGATIONS

63. Plaintiffs bring this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3),

and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All individuals whose PII was compromised in the data breach announced by Claire's on July 7, 2020 (the "Nationwide Class").

64. Additionally, Plaintiff Parker brings a Tennessee Subclass, defined as follows:

> All persons residing in Tennessee whose PII was compromised in the data breach announced by Claire's on July 7, 2020 (the "Tennessee Subclass").

65. Excluded from the Class are the following individuals and/or entities: Defendants and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

66. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

67. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendants have identified thousands of customers whose PII may have been improperly accessed in the data breach, and the Classes are apparently identifiable within Defendants' records.

68. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class members. These include:

a. When Defendants actually learned of the data breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class members' PII;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class members' PII;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

h. Whether Defendants caused Plaintiffs and Class members damages;

i. Whether Defendants violated the law by failing to promptly notify Class members that their PII had been compromised;

j. Whether Plaintiffs and the other Class members are entitled to credit monitoring and other monetary relief;

k. Whether Defendants violated the Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 ILCS § 505/1, *et seq.*, by failing to implement reasonable security procedures and practices;

l. Whether Defendants violated the Illinois Personal Information Protection Act, 815 ILCS § 530/1, *et seq.*, by failing to maintain reasonable security procedures and practices appropriate to the nature of the PII.

m. Whether Defendants violated Tennessee's Consumer Protection Act, Tenn. Code. Ann. § 47-18-101, *et seq.*, by failing to implement reasonable security procedures and practices;

69. **Typicality**: Plaintiffs' claims are typical of those of other Class members because all had their PII compromised as a result of the data breach, due to Defendants' misfeasance.

70. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests

of the Class members. Plaintiffs' Counsel are competent and experienced in litigating privacy-related class actions.

71. **Superiority and Manageability**: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

72. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

73. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiffs and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach; and

e. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

**FIRST CLAIM FOR RELIEF**
**Negligence**
**(On Behalf of Plaintiffs and the Nationwide Class)**

74. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

75. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

76. The legal duties owed by Defendants to Plaintiffs and Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and Class members in its possession;

b. To protect PII of Plaintiffs and Class members in its possession using reasonable and adequate security procedures 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, including promptly notifying Plaintiffs and Class members of the data breach.

77. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendants.

78. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiffs and Class members are consumers under the FTC Act.

Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

79. Defendants breached their duties to Plaintiffs and Class members. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the facts that "scraping" hacks have been surging since 2016.

80. Defendants knew or should have known that their security practices did not adequately safeguard Plaintiffs' and the other Class members' PII, including, but not limited to, the failure to detect the malware infecting Defendants' ecommerce platform for months.

81. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII of Plaintiffs and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PII during the period it was within Defendants' possession and control.

82. Defendants breached the duties they owe to Plaintiffs and Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the data breach (*e.g.*, There is no indication that Defendants' ecommerce platform is PCI DSS compliant and encrypts customers' order information, such as name, address, and credit card number, during data transmission, which did not occur here);

c. Failing to act despite knowing or having reason to know that Defendants' systems were vulnerable to E-skimming or similar attacks (*e.g.*, Defendants did not detect

the malicious code on the ecommerce platform, nor did they implement safeguards in light of the surge of E-skimming attacks on retailers); and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

83. Due to Defendants' conduct, Plaintiffs and Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class members. Hackers not only "scraped" many of Claire's customers' names from the website, they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and payment card expiration dates. They got the *fullz* – everything they need to illegally use Claire's customers' credit cards to make illegal purchases. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

84. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[18] Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

85. As a result of Defendants' negligence, Plaintiffs and Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the

[18] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring, but it only monitors victims' credit reports at one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession, subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiffs and Class members, including ongoing credit monitoring.

86. These injuries were reasonably foreseeable given the history of security breaches of this nature since 2016. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' negligent conduct.

**SECOND CLAIM FOR RELIEF**
**Declaratory Judgment**
**(On Behalf of Plaintiffs and the Nationwide Class)**

87. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

88. Defendants owe duties of care to Plaintiffs and Class members which would require it to adequately secure PII.

89. Defendants still possess PII regarding Plaintiffs and Class members.

90. Although Claire's claims it has "reinforced the security of our site," there is no detail on what, if any, fixes have really occurred.

91. Plaintiffs and Class members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

92. There is no reason to believe that Defendants' security measures are any more adequate than they were before the breach to meet Defendants' contractual obligations and legal duties, and there is no reason to think Defendants have no other security vulnerabilities that have not yet been knowingly exploited.

93. Plaintiffs, therefore, seek a declaration that (1) each Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and securing checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Class members for a period of ten years; and

h. Meaningfully educating its users about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendants' customers must take to protect themselves.

**THIRD CLAIM FOR RELIEF**
**Violations of the Tennessee Consumer Protection Act,**
**Tenn. Code. Ann. § 47-18-101, *et seq*.**
**(On Behalf of Plaintiff Parker and the Tennessee Subclass)**

94. Plaintiff Parker re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 73.

95. Tenn. Code Ann. § 47-18-109(a)(1) provides that "[a]ny person who suffers an ascertainable loss of money or property, real, personal, or mixed, or any other article, commodity, or thing of value wherever situated, as a result of the use or employment by another person of an unfair or deceptive act or practice described in § 47-18-104(b) and declared to be unlawful by this part, may bring an action individually to recover actual damage."

96. Tenn. Code Ann. § 47-18-109(a)(3) further provides that "[i]f the court finds that the use or employment of the unfair or deceptive act or practice was willful or knowing violation of this part, the court may award three (3) times the actual damages sustained and may provide such other relief as it considers necessary and proper…"

97. Defendants' online sales of jewelry and accessories constitute "trade or commerce."

98. Defendants' conduct violates the Tennessee Consumer Protection Act because Defendants engaged in the deceptive acts and practices described above, which included a failure to protect Plaintiff Parker's and the Subclass's PII in spite of assurances to the contrary.

99. Defendants omitted material facts concerning the steps they took (or failed to undertake) to protect Plaintiff Parker and Subclass members' PII, which were deceptive, false and misleading given the conduct described herein. Such conduct is inherently and materially deceptive and misleading in a material respect, which was known, or by the exercise of reasonable care, should have been known, to be untrue, deceptive or misleading by Defendants. Such conduct is unfair, deceptive, untrue, or misleading in that Defendants: (a) represented that

their services have approval, characteristics, uses or benefits that they do not have; and (b) represented that services are of a particular standard, quality or grade.

100. The materially misleading statements and deceptive acts and practices of Defendants alleged herein were directed at the public at large.

101. Defendants' actions impact the public interest because Plaintiff Parker and the Tennessee Subclass have been injured in exactly the same way as thousands of others as a result of and pursuant to Defendants' generalized course of deception as described throughout this Complaint.

102. Defendants' acts and practices described above were likely to mislead a reasonable consumer acting reasonably under the circumstances.

103. Defendants' misrepresentations, misleading statements and omissions were materially misleading to Plaintiff Parker and members of the Class.

104. Defendants' violation of Tenn. Code Ann. § 47-18-104 was willful and knowing. As described above, at all relevant times, Defendants, among other things, knew that their policies and procedures for the protection of Plaintiff Parker's and the Tennessee Subclass' PII were inadequate to protect that PII. Nonetheless, Defendants continued to solicit and process PII in the United States in order to increase their own profits.

105. Had Plaintiff Parker and the members of the Tennessee Subclass known of Defendants' misrepresentations, misleading statements and omissions about their use of PII, they would not have made online purchases at Defendants' website.

106. As a direct and proximate result of Defendants' conduct in violation of Tenn. Code Ann. § 47-18-104, Plaintiff Parker and the members of the Tennessee Subclass have been injured in amounts to be proven at trial.

107. As a result, pursuant to Tenn. Code Ann. §§ 47-18-104 and 47-18-109, Plaintiff Parker and the Tennessee Subclass are entitled to make claims against Defendants for ascertainable damages in an amount to be determined at trial. Plaintiff Parker also properly asks

that such damages be trebled based on Defendants' knowledge and/or intention with respect to their breach.

108. Plaintiff Parker also seek injunctive relief, including a robust, state of the art notice program for the wide dissemination of a factually accurate statement on the actual state of Defendants' PII storage and the implementation of a corrective advertising campaign by Defendants.

109. Additionally, pursuant to Tenn. Code Ann. § 47-18-109, Plaintiff Parker and the Tennessee Subclass make claims for attorneys' fees and costs.

## FOURTH CLAIM FOR RELIEF
**Unjust Enrichment**
**(On Behalf of Plaintiffs and the Nationwide Class)**

110. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

111. Plaintiffs and class members conferred a monetary benefit upon Defendants in the form of monies paid for goods available on Defendants' websites.

112. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and class members. Defendants also benefited from the receipt of Plaintiffs' and class members' PII, as this was utilized by Defendants to facilitate payment to them.

113. The monies for goods that Plaintiffs and class members paid to Defendants were to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

114. As a result of Defendants' conduct, Plaintiffs and class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and class members

paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

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

116. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and class members all unlawful or inequitable proceeds received by it as a result of the conduct alleged herein.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and all Class members, request judgment against the Defendants and that the Court grant the following:

A. An order certifying the Nationwide Class and Tennessee Subclass as defined herein, and appointing Plaintiffs and their counsel to represent the classes;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and Class members' PII;

C. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiffs and all Class members;

D. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as

allowable by law; and

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

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand that this matter be tried before a jury.

Date: September 18, 2020

Respectfully Submitted,

By: *Carl V. Malmstrom*

**WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC**
CARL MALMSTROM
malmstrom@whafh.com
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: 312/984-0000
Facsimile: 212/545-4653

**CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.**
M. ANDERSON BERRY
aberry@justice4you.com
LESLIE GUILLON
lguillon@justice4you.com
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829