☐ YES ☑ NO

EXHIBITS

CASE NO. 2020 CH 5218

DATE: 7/31/2020

CASE TYPE: Class Action

PAGE COUNT: 36

CASE NOTE

_____

_____

_____

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT – CHANCERY DIVISION

JULIA ROSSI, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CLAIRE'S STORES, INC.;
CBI DISTRIBUTING CORP.,

Serve Registered Agent:
[Registered Agent Solutions, 901 S. 2nd Street, Suite 201, Springfield, IL 62704]

Defendants.

Case No. 2020CH05218

(JURY TRIAL DEMANDED)

CLASS ACTION COMPLAINT

Plaintiff Julia Rossi ("Plaintiff"), individually and on behalf of all others similarly situated, alleges on personal knowledge, investigation of counsel, and on information and belief as follows:

SUMMARY OF THE CASE

1. This class action arises as a result of Defendants Claire's Stores, Inc. and CBI Distributing Corp. (collectively, "Defendants"), worldwide jewelry and fashion accessory retailers, permitting an unauthorized intrusion of their e-commerce websites that compromised the personal and financial information of their customers.

2. On or about June 12, 2020, Defendants first learned that they were experiencing a data breach that resulted in the unauthorized access, disclosure, acquisition, and/or use of unsecured personal and financial information from online customer purchases from at least April 7, 2020 through June 12, 2020 (the "Data Breach"). The compromised customer information

included, without limitation, first and last names, addresses, email addresses, phone numbers, payment card numbers, payment card expiration dates, payment card verification codes, and Claire's account passwords, as well as gift card numbers and gift card PINs, if applicable (collectively, "Personal Information"). As a result of the Data Breach, the security and privacy of Plaintiff's and Class Members' Personal Information was compromised.

3. After investigating the Data Breach, Defendants waited almost one full month, at minimum, to provide notice to their affected customers, including Plaintiff, via a data breach notification letter dated on or about July 7, 2020 (the "Notice Letter").

4. In addition to revealing the Personal Information compromised in the Data Breach, the Notice Letter characterizes the Data Breach as "computer code that had been added to our site by an unauthorized person" that "was capable of obtaining information entered by customers during the checkout process and sending that information out of our system." The Notice Letter further indicates that recipients are being notified "because you placed an order during a time the added code was present."

5. Plaintiff's and Class Members' unsecured Personal Information compromised in the Data Breach as a direct result of Defendants' acts and/or omissions included the types of personal and financial information that people consider extremely sensitive and private. This extremely sensitive data should have received the most rigorous protection available, but it did not.

6. Defendants were collecting and storing Plaintiff's and Class Members' sensitive and confidential Personal Information, which they knew consumers consider extremely private, and which is valuable to criminals and vulnerable to exfiltration. Defendants failed to take security precautions necessary to protect the Personal Information.

7. Because Defendants failed to take necessary security precautions, Plaintiff's and Class Members' Personal Information was disclosed and exfiltrated by unauthorized persons, who now have been and will continue to be able to sell the compromised Personal Information for financial fraud and identity theft purposes.

8. It appears it was not difficult for a thief or a hacker to exploit Defendants' lax security and exfiltrate the Personal Information right under Defendants' noses, as Defendants failed to discover the intrusion for over one month and then waited roughly another month, at minimum, before providing any notice to the affected customers.

PARTIES

9. Plaintiff Julia Rossi is an individual residing in Dauphin County, Pennsylvania.

10. Defendant Claire's Stores, Inc. is a Florida corporation with its principal place of business in Hoffman Estates, Illinois. As self-described on its website, Claire's Stores, Inc. is "one of the world's leading specialty retailers of fashionable jewelry and accessories."[1]

11. 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 e-commerce websites where the Data Breach occurred.

JURISDICTION AND VENUE

12. This is a class action complaint for violations of state statutory and common law, seeking statutory and actual damages.

[1] https://www.clairestores.com/company-profile/company-overview.

13. No federal question is presented by this complaint. Plaintiff brings this complaint solely under state law and not under federal law, and specifically not under the United States Constitution, nor any of its amendments, nor under 42 U.S.C. § 1981 or 1982, nor any other federal statute, law, rule, or regulation. Plaintiff believes and alleges that a cause of action exists under state law for the conduct complained of herein.

14. Venue is proper under 735 ILCS 5/1-108 and 2-101 of the Illinois Code of Civil Procedure, as a substantial portion of the transactions giving rise to the causes of action pleaded herein occurred in Cook County. Specifically, upon information and belief, Defendants' unlawful conduct as alleged herein occurred in Cook County, Illinois, where Defendants' principal places of business are located.

STATEMENT OF FACTS

A. Defendants' Data Breach and Subsequent Notice to Affected Customers

15. Defendants are a large retail and online seller of jewelry and other fashion accessories. Defendants operate in over 40 countries, with over 2,000 retail locations in North America and Europe and over 7,000 store locations in the rest of the world.[2]

16. Between 2014 and 2017, Defendants' net sales reportedly averaged nearly $1.4 billion annually. In 2019 alone, Defendants' global net sales for online purchases through their websites—claires.com and icing.com—reportedly were $12.9 million.

17. In or around June 2020, reports surfaced that Defendants had recently experienced a cyber intrusion on their e-commerce platform by hackers utilizing Magecart tactics.[3] These

---

[2] *Id.*

[3] *See, e.g.*, Mathew J. Schwartz, *Claire's: Magecart E-Commerce Hackers Stole Card Data*, BANKINFO SECURITY, June 15, 2020, https://www.bankinfosecurity.com/claires-says-magecart-e-commerce-hackers-stole-card-data-a-14436.

hackers reportedly infiltrated Defendants' Salesforce Commerce Cloud environment for at least seven weeks.[4]

18. Upon information and belief, Defendants did not issue a press release regarding the Data Breach but confirmed the Data Breach through press inquiries.

19. The Data Breach resulted in the unauthorized access, disclosure, acquisition, and/or use of the Personal Information of Plaintiff and Class Members. In particular, the hackers added computer code to Defendants' e-commerce websites that obtained full payment card details and other Personal Information entered by customers during the checkout process and exfiltrated that information out of Defendants' systems and into the hands of unauthorized persons.

20. As a result of the Data Breach, the security and privacy of Plaintiff's and Class Members' Personal Information, including sensitive financial information, was compromised.

21. Although Defendants knew of the Data Breach no later than June 12, 2020 (and likely earlier), Defendants took no steps to notify customers whose information was compromised until on or about July 7, 2020, when Defendants began mailing Notice Letters to the affected individuals directly.

22. To date, Defendants' websites do not contain any information or notice regarding the Data Breach. Defendants' online "Press Room" also contains no reference to the Data Breach.[5]

23. The Notice Letter indicated, in part, the following:

> Claire's and Icing are writing to let you know that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.
>
> **What Happened?**

---

[4] *Id.*
[5] https://www.clairestores.com/financial-press-release.

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 [XXXX]. 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.
- **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 the email address).

24. Further, Defendants' Notice Letter acknowledged the very real threat that the incident would result in identity theft, fraud, and other similar risks by further encouraging recipients—Plaintiff and Class Members—to "closely review your payment card account statements for any unauthorized charges." The Notice Letter also instructed victims to "immediately report any unauthorized charges to the bank that issued your card . . . ."

25. Defendants also acknowledged their failure to safeguard customers' Personal Information, concluded the Notice Letter with an apology: "We regret that this occurred and apologize for any inconvenience."

26. Defendants' own statements confirm that Plaintiff and Class Members are subject to continued, future risk of identity theft, fraudulent charges, and other damages. Further, Defendants offered only one year of identity theft insurance, a level and duration of protection both woefully inadequate to address the risk of identity theft and fraud Defendants created by allowing the Data Breach to occur.

27. By acknowledging the exfiltration of Personal Information in the Notice Letter, Defendants reasonably believe and concede that Plaintiff's and Class Members' unencrypted Personal Information was acquired and viewed by unauthorized persons as a result of the Data Breach.

28. Further, Defendants reasonably believe and concede security, confidentiality, and/or integrity of Plaintiff's and Class Members' unencrypted Personal Information was compromised by Defendants as a result of the Data Breach.

29. It is reasonable to infer and should be rebuttably presumed that Plaintiff's and Class Members' unencrypted Personal Information that was acquired by unauthorized persons as a result of the Data Breach was viewed by unauthorized persons.

30. After receiving the Notice Letter, it is reasonable for recipients—Plaintiff and Class Members—to believe that future harm (including identity theft) is real and imminent, and for them to take steps to mitigate that risk of future harm.

B. Defendants Had an Obligation to Protect Personal Information Under the Applicable Law and Standard of Care.

31. Defendants had obligations created and imposed by state laws, and based on industry standards, to keep the compromised Personal Information confidential and to protect it from unauthorized disclosure. Plaintiff and Class Members provided their Personal Information to Defendants with the common sense understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized disclosure.

32. Defendants' data security obligations and promises were particularly important given the substantial increase in data breaches—particularly those in the retail industry—which were widely known to the public and to anyone in Defendants' industry.

33. Defendants' security failures demonstrate that they failed to honor their duties and promises by not maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks, adequately protecting Plaintiff's and Class Members' Personal Information, ensuring the confidentiality and integrity of the electronic Personal Information of customers, implementing technical policies and procedures for electronic information systems that maintain customers' Personal Information to allow access only to those persons or software programs that have been granted access rights, implementing policies and procedures to prevent, detect, contain, and correct security violations, implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, protecting against any reasonably anticipated threats or hazards to the security or integrity of customers' Personal Information, and training all members of their workforce effectively on the policies and procedures with respect to protecting customers' Personal Information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of customers' Personal Information.

34. As described before, Defendants also are required (by various other states' laws and regulations) to protect Plaintiff's and Class Members' Personal Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

35. In addition to their obligations under state laws, Defendants owed a duty to Plaintiff and Class Members, whose Personal Information was entrusted to Defendants, to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting the Personal Information in their possession from being compromised, lost, stolen, disclosed, accessed, viewed, and/or misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the Personal Information of Plaintiff and Class Members.

36. Defendants owed a duty to Plaintiff and Class Members, whose Personal Information was entrusted to Defendants, to design, maintain, and test their computer systems to ensure that the Personal Information in Defendants' possession was adequately secured and protected.

37. Defendants owed a duty to Plaintiff and Class Members, whose Personal Information was entrusted to Defendants, to create and implement reasonable data security practices and procedures to protect the Personal Information in their possession, including adequately training their employees and others who accessed Personal Information within their computer systems on how to adequately protect Personal Information.

38. Defendants owed a duty to Plaintiff and Class Members, whose Personal Information was entrusted to Defendants, to implement processes that would detect a breach or leak on their data security systems in a timely manner.

39. Defendants owed a duty to Plaintiff and Class Members, whose Personal Information was entrusted to Defendants, to act upon data security warnings and alerts in a timely fashion.

40. Defendants owed a duty to Plaintiff and Class Members, whose Personal Information was entrusted to Defendants, to adequately train and supervise their employees to detect a breach or leak on their data security systems in a timely manner.

41. Defendants owed a duty to Plaintiff and Class Members, whose Personal Information was entrusted to Defendants, to disclose if their computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' Personal Information from exfiltration or leaks because such an inadequacy would be a material fact in the decision to entrust Personal Information to Defendants.

42. Defendants owed a duty to Plaintiff and Class Members, whose Personal Information was entrusted to Defendants, to disclose in a timely and accurate manner when data breaches or leaks occurred.

43. Defendants owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

C. It is Well Established That Data Breaches Lead to Identity Theft and Other Harms.

44. Plaintiff and Class Members have been injured by the release, disclosure, and exfiltration of their Personal Information in the Data Breach.

45. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[6] Cyber criminals can leverage Plaintiff's and Class Members' Personal Information that was released, disclosed, and exfiltrated in the Data Breach to commit thousands of crimes, including opening new financial accounts in Plaintiff's and Class Members' names, taking out loans in Plaintiff's and Class Members' names, using Plaintiff's and Class Members' Personal Information to file fraudulent tax returns, using Plaintiff's and Class Members' information to obtain government benefits, obtaining driver's licenses in Plaintiff's and Class Members' names but with another person's photograph, giving false information to police during an arrest, and, of course, utilizing Plaintiff's and Class Members' payment card information to make any number of fraudulent purchases. Even worse, Plaintiff and Class Members could be arrested for crimes identity thieves have committed.

46. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

47. This is not just speculative. As the FTC has reported, if hackers get access to Personal Information, they **will** use it.[7]

48. Further, even if only some Personal Information is obtained by identity thieves, that information can be successfully utilized when aggregated or combined with other sensitive identifying information to form a complete "profile" of the victim, ripe for identity theft. If cyber

---

[6] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").
[7] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N, May 24, 2017, https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

criminals manage to acquire Personal Information, including financial information such as credit and debit card numbers, along with other sensitive information, such as Social Security numbers, driver's licenses, or passport numbers, there is no limit to the amount of fraud to which Defendants have exposed Plaintiff and Class Members.

49. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[8] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

50. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[9]

51. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

52. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, ***stolen data may be held for up to a year or more before being used to commit identity theft***. Further, once

---

[8] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), U.S. GOV'T ACCOUNTABILITY OFFICE, June 2007, https://www.gao.gov/new.items/d07737.pdf.
[9] *Id.* at 2, 9.

> stolen data have been sold or posted on the Web, ***fraudulent use of that information may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

53. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account; they can also commit all manners of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's Personal Information to obtain government benefits; or, filing a fraudulent tax return using the victim's Personal Information.[11]

54. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers and other Personal Information directly on various Internet websites making the information publicly available.

55. Furthermore, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[12]

56. To date, Defendants do not appear to be taking any measures to assist Plaintiff and Class Members other than telling them to simply do the following:

- "review your payment card account statements regularly for any unauthorized charges";
- "report any unauthorized charges to your bank"; and

---

[10] *Id*. at 29 (emphases added).
[11] *Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.
[12] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, Sept. 2013, https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

- offering one year of identity theft insurance.

None of these recommendations or offers, however, require Defendants to expend any material effort, or take reasonable measures, to protect Plaintiff's and Class Members' Personal Information.

57. Defendants' failure to adequately protect Plaintiff's and Class Members' Personal Information has resulted in Plaintiff and Class Members having to undertake protective and mitigating measures, which require extensive amounts of time, calls, and, for many of the more adequate credit and fraud protection services, payment of money—while Defendants sit by and do nothing to assist those affected by the Data Breach. Instead, as Defendants' Notice Letter indicates, they are placing the burden on Plaintiff and Class Members to discover and rectify fraudulent activity and identity theft.

58. Defendants' offer of twelve months of "Internet surveillance" and identity theft insurance is woefully inadequate. While some harm has already begun to occur, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Personal Information); it does not prevent identity theft.[13]

59. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud

[13] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

and identity theft. Plaintiff and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

60. Plaintiff and the Class Members have suffered, continue to suffer and/or will suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper release and disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Deprivation of the value of Plaintiff's and Class Members' Personal Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

61. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards.

D. Plaintiff's Experience

62. Defendants received and collected Plaintiff's Personal Information when she purchased merchandise from Defendants' websites, which Defendants maintained in their computer systems. Defendants then disclosed Plaintiff's Personal Information to unauthorized third parties as a result of the Data Breach.

63. In July 2020, Plaintiff received a Notice Letter dated July 7, 2020 from Marie Hodge, Defendants' Executive Director of Communications and Operations, notifying Plaintiff of the Data Breach. The contents of the Notice Letter are the same as those previously alleged herein.

64. Since June 2020, Plaintiff has experienced a substantial increase in spam/phishing calls from persons apparently attempting to defraud her. In many instances, these fraudulent callers leave threatening or otherwise deceptive voice messages in an attempt to obtain additional Personal Information from Plaintiff.

65. Prior to the Data Breach, Plaintiff was not regularly receiving spam/phishing calls. Since the Data Breach occurred, Plaintiff has been receiving these calls on a daily basis, often multiple calls per day.

66. Plaintiff now engages in daily monitoring of her financial accounts for fraudulent activity, including, without limitation, the account compromised in the Data Breach. She also has requested copies of her credit reports and has spent significant time reviewing those reports for signs of fraudulent credit activity.

67. Plaintiff has spent several hours per day of her own time since learning of the Data Breach attempting to mitigate the risks of fraud and identity theft created by Defendants so that she does not become further victimized because of the Data Breach. Further, Plaintiff now spends significant time on a daily basis dealing with a high volume of phishing calls and voice messages.

68. As the recipient of the Notice Letter from Defendants, it is and was reasonable for Plaintiff to believe that future harm (including fraudulent charges and identity theft) is and was real and imminent, and to take steps to mitigate that risk of future harm.

69. Had Plaintiff known that Defendants were not maintaining customers' Personal Information with adequate security and that Defendants' systems were susceptible to data breaches, Plaintiff would not have provided her Personal Information to Defendants to purchase merchandise on Defendants' websites.

70. Further, a portion of the price Plaintiff paid for the merchandise she purchased on Defendants' websites, like all other revenue Defendants obtained from customers, was or should have been allocated by Defendants to adequately safeguard customers' Personal Information, but it was not. Thus, Plaintiff and Class Members overpaid for the online merchandise they purchased from Defendants and should be entitled to restitution for that overpayment.

CLASS ALLEGATIONS

71. Plaintiff brings this class action lawsuit pursuant to 735 ILCS 5/2-801, individually and on behalf of all others similarly situated.

72. Plaintiff seeks certification of a Nationwide Class and a Pennsylvania Sub-Class (collectively, the "Class") defined as follows:

> Nationwide Class: All persons in the United States whose Personal Information was compromised as a result of the Data Breach disclosed by Defendants on or about July 7, 2020.
>
> Pennsylvania Sub-Class: All persons in the Commonwealth of Pennsylvania whose Personal Information was compromised as a result of the Data Breach disclosed by Defendants on or about July 7, 2020.

73. Specifically excluded from the Class are Defendants and any entities in which Defendants have a controlling interest, Defendants' agents and employees, the judge to whom this action is assigned, members of the judge's staff, and the judge's immediate family.

74. **Numerosity:** Plaintiff does not know the exact number of Class Members but is informed and believes the Class comprises many thousands of individuals throughout the United States. As such, Class Members are so numerous that joinder of all members is impracticable.

75. **Commonality and Predominance:** Common questions of law and fact exist and predominate over any questions affecting only individual Class Members. The common questions include:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants failed to adequately safeguard Plaintiff's and Class Members' Personal Information;

c. Whether Defendants failed to protect Plaintiff's and Class Members' Personal Information properly and/or as promised;

d. Whether Defendants' computer system and data security practices used to protect Plaintiff's and the Class Members' Personal Information violated applicable state law, and/or Defendants' duties to safeguard the information;

e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Personal Information;

f. Whether Defendants violated the consumer protection statutes and/or data breach notification statutes applicable to Plaintiff and Class Members;

g. Whether Defendants failed to notify Plaintiff and Class Members about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

h. Whether Defendants acted negligently in failing to safeguard Plaintiff's and Class Members' Personal Information;

i. Whether Defendants breached their express or implied contractual obligations to protect the confidentiality of Plaintiff's and the Class Members' Personal Information, and to have reasonable data security measures;

j. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct;

l. What equitable relief is appropriate to redress Defendants' wrongful conduct; and

m. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members.

76. **Typicality:** Plaintiff's claims are typical of the claims of the other Class Members. Plaintiff and Class Members were injured through Defendants' uniform misconduct and their legal claims arise from the same core practices of Defendants.

77. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

78. **Superiority:** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class Member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendants. Even if it were economically feasible, requiring each affected Class Member to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Plaintiff anticipates no unusual difficulties in managing this class action.

COUNT I
Negligence

79. Plaintiff incorporates herein every previously alleged factual allegation.

80. This count is brought on behalf of the National Class or, in the alternative, the Pennsylvania Sub-Class.

81. Defendants solicited, collected, and stored the Personal Information of Plaintiff and Class Members.

82. Defendants knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and Class Members' Personal Information and the importance of adequate security.

83. Defendants were well aware of the fact that hackers routinely attempt to access Personal Information without authorization. Defendants also knew about numerous, well-publicized data breaches wherein hackers stole the Personal Information from other retailers who held or stored such information.

84. Defendants owed duties of care to Plaintiff and Class Members whose Personal Information had been entrusted with Defendants.

85. Defendants owed a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and Class Members when obtaining, storing, using, and managing their Personal Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize or avoid losses.

86. This duty extends to protecting others from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard Personal Information.

87. Plaintiff and Class Members were the intended beneficiaries of Defendants' duty to safeguard their Personal Information, creating a special relationship between them and

Defendants. Only Defendants were in a position to ensure that their systems were sufficient to protect Plaintiff's and Class Members' Personal Information that was entrusted to them.

88. Defendants also were subject to an independent duty to safeguard Plaintiff's and Class Members' Personal Information that was untethered to any contract between Defendants and Plaintiff and Class Members.

89. In addition to the general duties above, Defendants' duties specifically included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting Personal Information in their possession;

b. To protect Personal Information in their possession using reasonable and adequate security procedures and systems;

c. To adequately and properly audit, test, and train their employees regarding how to properly and securely transmit and store Personal Information;

d. To implement processes to quickly detect a data breach, security incident, or intrusion; and

e. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

90. It was foreseeable that injury to Plaintiff and Class Members would result from Defendants' violation of these duties in mishandling Plaintiff's and Class Members' Personal Information.

91. Because Defendants knew that a security incident, breach, or intrusion upon their systems would potentially damage hundreds of thousands of individuals, including Plaintiff and Class Members, Defendants had a duty to adequately protect their Personal Information.

92. Defendants knew, or should have known, that their security practices and computer systems did not adequately safeguard Plaintiff's and Class Members' Personal Information.

93. Defendants breached their duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard Plaintiff's and Class Members' Personal Information.

94. Defendants breached their duties of care by failing to provide prompt notice of the Data Breach to Plaintiff and Class Members.

95. Defendants acted with reckless disregard for the security of Plaintiff's and Class Members' Personal Information because Defendants knew or should have known that their computer systems and data security practices were not adequate to safeguard the Personal Information that they collected and stored.

96. Defendants acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate notice of the Data Breach so they could take measures to protect themselves from damages caused by the fraudulent use of Personal Information compromised in the Data Breach.

97. Defendants had a special relationship with Plaintiff and Class Members. The willingness to share and entrust Plaintiff's and Class Members' Personal Information with Defendants was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the Personal Information stored therein) and to implement security practices to protect the Personal Information they collected and stored.

98. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Personal Information. Defendants' misconduct included failing to:

a. Secure access to their servers;

b. Comply with current industry standard security practices;

c. Properly and adequately train employees on proper data security practices;

d. Implement adequate system and event monitoring;

e. Implement the systems, policies, and procedures necessary to prevent hackers from accessing and utilizing Personal Information transmitted and/or stored by Defendants;

f. Undertake periodic audits of record-keeping processes to evaluate the safeguarding of Personal Information;

g. Secure Personal Information and limit access to it to those with a legitimate business need;

h. Employ or contract with trained professionals to ensure security of network servers and evaluate the systems used to manage e-mail, Internet use, and so forth; and

i. Have a plan ready and in position to act quickly should a theft or data breach occur.

99. Defendants also had independent duties under state law requiring it to reasonably safeguard Plaintiff's and Class Members' Personal Information and promptly notify them about the Data Breach.

100. Defendants breached the duties they owed to Plaintiff and Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' Personal Information both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards before, during, and after the period of the Data Breach; and

d. By failing to timely and accurately disclose that Plaintiff's and Class Members' Personal Information had been improperly disclosed, accessed, viewed, released, acquired, and used in the Data Breach.

101. But for Defendants' wrongful and grossly negligent breach of the duties Defendants owed Plaintiff and Class Members, their Personal Information either would not have been compromised or they would have been able to prevent some or all of their damages.

102. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of certainly impending future harm.

103. The injury and harm Plaintiff and Class Members suffered, as alleged above, was and is reasonably foreseeable.

104. The injury and harm Plaintiff and Class Members suffered, as alleged above, was the direct and proximate result of Defendants' negligent conduct.

105. Plaintiff and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract

106. Plaintiff incorporates herein every previously alleged factual allegation.

107. This count is brought on behalf of the National Class or, in the alternative, the Pennsylvania Sub-Class.

108. When Plaintiff and Class Members provided their Personal Information to Defendants in exchange for Defendants' products, they entered into implied contracts with Defendants under which—and by mutual assent of the parties—Defendants agreed to take reasonable steps to protect their Personal Information.

109. Defendants solicited and invited Plaintiff and Class Members to provide their Personal Information as part of Defendants' regular business practices and as essential to the sales transaction process for card payment transactions. This conduct thus created implied contracts between Plaintiff and Class members on one hand, and Defendants on the other hand. Plaintiff and Class Members accepted Defendants' offers by providing their Personal Information to Defendants in connection with purchases on Defendants' websites.

110. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards.

111. Defendants' implied promise to safeguard Plaintiff's and Class Members Personal Information is evidenced by a duty to protect and safeguard Personal Information that Defendants required Plaintiff and Class Members to provide as a condition of entering into credit and debit card transactions with Defendants.

112. Plaintiff and Class Members paid money to Defendants to purchase items at Defendants' websites. Plaintiff and Class Members reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

113. Plaintiff and Class Members, on the one hand, and Defendants, on the other hand, mutually intended—as inferred from customers' continued use of Defendants' card payments system to make purchases—that Defendants would adequately safeguard Personal Information. Defendants failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Class Members.

114. Plaintiff and Class Members value data security and would not have provided their Personal Information to Defendants in the absence of Defendants' implied promise to keep the Personal Information reasonably secure.

115. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

116. Defendants breached their implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

117. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

118. Plaintiff and Class Members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

119. Plaintiff and Class Members also are entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, submit to future periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
Unjust Enrichment

120. Plaintiff incorporates herein every previously alleged factual allegation.

121. This count is brought in the alternative to Plaintiff's breach of implied contract count.

122. This count is brought on behalf of the National Class or, in the alternative, the Pennsylvania Sub-Class.

123. Plaintiff and Class Members conferred a monetary benefit on Defendants. Defendants received and retained money belonging to Plaintiff and Class Members directly through purchased made on Defendants' websites.

124. Defendants had knowledge of the benefits conferred on it by Plaintiff and Class Members.

125. The money that Plaintiff and Class Members paid directly to Defendants was supposed to be used by Defendants, in part, to pay for the costs of reasonable data privacy and security practices and procedures for the collection, storage, and use of Plaintiff's and Class Members' Personal Information.

126. As a result of Defendants' conduct, Plaintiff and Class Members suffered damages in an amount equal to the difference in value between the online transactions with the reasonable data privacy and security practices and procedures for which they paid, and the transactions without reasonable data privacy and security practices and procedures that they actually received.

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

128. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendants received.

129. A constructive trust should be imposed on all unlawful or inequitable sums received by Defendants traceable to Plaintiff and Class Members.

COUNT IV
Violations of the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

130. Plaintiff incorporates herein every previously alleged factual allegation.

131. This count is brought on behalf of the National Class.

132. Plaintiff and Class Members provided their Personal Information to Defendants in order to make purchases on Defendants' websites.

133. The Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*. ("PIPA") requires that businesses that maintain or store Personal Information such as that provided by Plaintiff and Class Members must provide immediate notification to the owners or licensees of such data in the event of a security breach, and cooperate with the owners and licensees thereafter.

134. Under 815 ILCS 530/5, Defendants are, and at all relevant times were, "data collectors" in that they are private corporations or retail operators that for any purpose "handle, disseminate, or otherwise deal with nonpublic personal information." Specifically, Defendants were and are data collectors that maintained or stored, but did not own or license, the computerized data that included the Personal Information of Plaintiff and Class Members.

135. The Personal Information obtained from Plaintiff and Class Members by Defendants was "personal information" under 815 ILCS 530/5 as it contained Plaintiff's and each Class Members' first name or initial, and last name, in combination with a credit or debit card number.

136. At all relevant times, Plaintiff and Class Members were the owners or licensees of their respective Personal Information.

137. As alleged herein, Defendants were the subjects of a "breach of the security of the system data" owned, operated, or controlled by Defendants under 815 ILCS 530/5.

138. Defendants, as data collectors that maintained or stored, but did not own or license, computerized data containing the Personal Information of Plaintiff and Class Members, and had suffered a breach of their security of the system data, was required pursuant to 815 ILCS 530/10(b) to notify Plaintiff and Class Members immediately of the Data Breach upon discovering it.

139. Defendants violated 815 ILCS 530/10(b) by failing to promptly notify Plaintiff and Class Members of the Data Breach, instead waiting nearly one month to start sending out the Notice Letters.

140. It was foreseeable that Defendants' failure to comply with PIPA would subject Plaintiff and Class Members to the risk that their Personal Information would be further compromised by unauthorized third parties, and Defendants unlawful conduct did, in fact, result in such additional compromising.

141. The damages sustained by Plaintiff and Class Members as described herein were the actual and proximate result of Defendants' violations of PIPA.

COUNT V
Violations of the Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 ILCS § 505/1, *et seq.*

142. Plaintiff incorporates herein every previously alleged factual allegation.

143. This count is brought on behalf of the National Class.

144. As a result of Defendants' unlawful conduct alleged herein, Defendants violated 815 ILCS § 505/1, *et seq.* by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and Class Members' Personal Information.

145. Further, Defendants' violation of PIPA, 815 ILCS § 530/10(b), as alleged herein, constitutes an "unlawful practice" under 815 ILCS § 505/1, *et seq.* pursuant to 815 ILCS § 530/20.

146. Plaintiff and Class Members suffered damages as a direct and proximate result of Defendants' unlawful conduct in violation of 815 ILCS § 505/1, *et seq.*

147. Plaintiff, individually and on behalf of all Class Members, seeks all remedies available under 815 ILCS § 505/1, *et seq.*

COUNT VI
Violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 201-1, *et seq.*

148. Plaintiff incorporates herein every previously alleged factual allegation.

149. This count is brought on behalf of the Pennsylvania Sub-Class.

150. Plaintiff, Class Members, and Defendants are "persons" as defined by 73 Pa. Stat. § 201-2(2).

151. Plaintiff and Class Members purchased goods and services in "trade" and "commerce" as defined by 73 Pa. Stat. § 201-2(3).

152. Plaintiff and Class Members purchased goods and services primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

153. Defendants engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined by 73 Pa. Stat. § 201-2(4) by, among other things, engaging in the following conduct:

a. Representing that their goods and services had characteristics, uses, benefits, and qualities that they did not have – namely that their goods, services, and business practices were accompanied by adequate data security (73 Pa. Stat. § 201-2(4)(v));

b. Representing that their goods and services were of a particular standard or quality when they were of another standard or quality (73 Pa. Stat. § 201-2(4)(vii));

c. Advertising their goods and services with intent not to sell them as advertised (73 Pa. Stat. § 201-2(4)(ix)); and

d. "Engaging in any other . . . deceptive conduct which creates a likelihood of confusion or of misunderstanding" (73 Pa. Stat. § 201-2(4)(xxi)).

154. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by 73 Pa. Stat. § 201-3.

155. Defendants' unfair or deceptive acts and practices include but are not limited to: failing to implement and maintain reasonable data security measures to protect Personal Information; failing to identify foreseeable data security risks and remediate the identified risks; failing to comply with common law duties, industry standards, and FTC guidance regarding data security; and omitting and concealing the material fact that it did not have reasonable measures in place to safeguard such Personal Information.

156. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security practices and ability to protect customers' Personal Information.

157. Defendants intended to mislead consumers and induce them to rely on their misrepresentations and omissions, and Plaintiff and Class Members did rely on Defendants' misrepresentations and omissions relating to their data privacy and security.

158. Plaintiff and Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

159. Had Defendants disclosed to consumers that their data security systems were not secure and, thus, were vulnerable to attack, Plaintiff and Class Members would not have given their Personal Information to Defendants.

160. Defendants acted intentionally, knowingly, and maliciously in violating 73 Pa. Stat. § 201-1, *et seq.*, and recklessly disregarded consumers' rights.

161. As a direct and proximate result of Defendants violation of violating 73 Pa. Stat. § 201-1, *et seq.*, Plaintiff and Class Members have suffered and will continue to suffer damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as alleged herein.

162. Plaintiff and Class Members seek all remedies available under violating 73 Pa. Stat. § 201-1, *et seq.*, including, but not limited to, the damages expressly permitted under 73 Pa. Stat. § 201-9.2: actual damages or statutory damages of $100, whichever is greater, treble damages defined as three time the actual damages, reasonable attorneys' fees and litigation costs, and any other such additional relief the Court deems necessary or proper.

163. Plaintiff and Class Members also seek injunctive relief as set forth herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, respectfully requests the Court order relief and enter judgment in her favor and against Defendants as follows:

A. An order certifying this action as a class action, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein.

B. Plaintiff requests injunctive and other equitable relief as is necessary to protect the interests of the Class, including (i) an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein; (ii) requiring Defendants to protect all data collected or received through the course of their business in accordance with applicable law and best practices under industry standards; (iii) requiring Defendants to design, maintain, and test their computer systems to ensure that Personal Information in their possession is adequately secured and protected; (iv) requiring Defendants to disclose any future data breaches in a timely and accurate manner; (v) requiring Defendants to engage third-party security auditors 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 them to promptly correct any problems or issues detected by these auditors; (vi) requiring Defendants to audit, test, and train their security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii) requiring Defendants to implement multi-factor authentication requirements; (viii) requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices; (ix) requiring Defendants to encrypt all Personal Information; (x) requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures; (xi) requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems; (xii) requiring Defendants to purge, delete, and destroy in a reasonably secure and timely manner Personal

Information no longer necessary for their provision of services; (xiii) requiring Defendants to conduct regular database scanning and securing checks; (xiv) requiring Defendants to routinely and continually conduct 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; (xv) requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Class Members; and (xvi) requiring Defendants to educate all Class Members about the threats they face as a result of the loss of their Personal Information to third parties, as well as steps Class Members must take to protect themselves.

C. A judgment awarding Plaintiff and Class Members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement;

D. An order that Defendants pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

E. Pre-judgment and post-judgment interest;

F. Attorneys' fees, expenses, and the costs of this action; and

G. All other and further relief as this Court deems necessary, just, and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Respectfully submitted,

Dated: July 31, 2020

/s/ Katrina Carroll

Katrina Carroll
kcarroll@carlsonlynch.com
Kyle A. Shamberg
kshamberg@carlsonlynch.com
CARLSON LYNCH LLP
111 West Washington Street, Suite 1240
Chicago, Illinois 60602
Telephone: (312) 750-1265
Firm ID: 63746

Tina Wolfson
twolfson@ahdootwolfson.com
Henry Kelston
hkelston@ahdootwolfson.com
Bradley K. King
bking@ahdootwolfson.com
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: (310) 474-9111
Fax: (310) 474-8585

Counsel for Plaintiff and the Proposed Class