Benjamin Heikali (SBN 307466)
E-mail: bheikali@faruqilaw.com
Joshua Nassir (SBN 318344)
E-mail: jnassir@faruqilaw.com
FARUQI & FARUQI, LLP
10866 Wilshire Boulevard, Suite 1470
Los Angeles, CA 90024
Telephone: (424) 256-2884
Facsimile: (424) 256-2885

Attorneys for Plaintiff Rosalie Golbahar

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

ROSALIE GOLBAHAR, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SHEIN FASHION GROUP, INC., a California corporation,

Defendant.

Case No.: 2:18-cv-10340

CLASS ACTION COMPLAINT

1. **Breach of Implied Contract;**
2. **Negligence;**
3. **Violations of Cal. Civ. Code § 1798.81.5;**
4. **Negligence Per Se;**
5. **Unjust Enrichment;**
6. **Declaratory Judgment; and**
7. **Violation of California Business and Professions Code §§ 17500, *et seq.***

JURY TRIAL DEMANDED

Plaintiff Rosalie Golbahar ("Plaintiff"), by and through her counsel, brings this Class Action Complaint against SHEIN Fashion Group, Inc. ("SHEIN") on behalf of herself and all others similarly situated, and alleges upon personal knowledge as to her own actions, and upon information and belief as to counsel's investigations and all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this consumer class action against SHEIN, a prominent fashion e-commerce platform, for its failures to secure and safeguard its customers' private information, including their email addresses and passwords ("Customer Data") of those who created accounts on the SHEIN website.

2. On August 22, 2018, SHEIN discovered that the Customer Data was stolen by hackers, resulting in the unauthorized access of at least 6.42 million users (the "Data Breach").[1] The Data Breach was active from around June 2018 to early August 2018.[2]

3. SHEIN only announced the Data Breach a month later on September 21, 2018 but provided little technical detail to customers or the public about how the Data Breach occurred.[3] According to SHEIN, hackers had obtained access to the Customer Data through "back door" entry points to the SHEIN servers.[4] Despite promises to do otherwise, SHEIN has yet provide any further information regarding the Data Breach.

4. Since the Data Breach, SHEIN has eliminated any reference or notification of the breach from the homepage of the SHEIN website, likely due to the potential negative impact such notice would have on potential shoppers during the

---

[1] https://www.prnewswire.com/news-releases/shein-notifies-customers-who-may-have-been-affected-by-data-breach-300717103.html (last visited on December 13, 2018).

[2] *Id.*

[3] *Id.*

[4] *Id.*

holiday season.

5. While SHEIN claims it has not seen evidence that credit card information was stolen in the Data Breach, SHEIN could not definitely disclaim that credit card information was not stolen because SHEIN "***typically*** does not store credit card information on its systems."[5] (emphasis added). Moreover, in its privacy policy, SHEIN claims that "[i]f you make a purchase, we collect personal data in connection with the purchase. This data includes your payment data, such as your credit or debit card number and other card information, and other account and authentication information, as well as billing, shipping, and contact details."[6]

6. Furthermore, with the known Customer Data stolen, criminals can engage in "credential stuffing," a type of cyberattack where stolen account credentials (typically usernames, emails, and passwords) are used to gain unauthorized access to a user's other online accounts through large-scale automated login requests directed against a web application.[7] This can result in the unauthorized access to other personal data store on those online accounts, such as payment card data, social security numbers, driver license numbers, and addresses. This is precisely what happened with Plaintiff's Customer Data.

7. In addition to SHEIN's failure to prevent or detect the Data Breach for about two months, SHEIN chose to remain silent upon discovering the Data Breach, waiting one month before disclosing the breach to its customers or the public. Plaintiff was not notified of the Data Breach until she received a letter from SHEIN dated October 1, 2018.

---

[5] https://us.shein.com/datasecurity?ref=www&rep=dir&ret=us (last visited December 13, 2018).

[6] https://us.shein.com/Privacy-Security-Policy-a-282.html (last visited on December 13, 2018).

[7] https://www.owasp.org/index.php/Credential_stuffing (last visited on December 13, 2018).

8. Had SHEIN detected the Data Breach earlier, less data would have been stolen and customers would have been able to take earlier action to mitigate their damages.

9. For these reasons, SHEIN disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable data-security measures to ensure its systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to monitor and detect the breach on a timely basis, and failing to disclose to its customers the material facts that it did not have adequate security systems and practices to safeguard Customer Data.

10. The private Customer Data obtained from the data breach was compromised due to SHEIN's acts and omissions and its failure to properly protect the Customer Data. If SHEIN had maintained and implemented proper data-security measures to safeguard Customer Data, deter the criminal hackers that orchestrated the Data Breach, and detect the breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented, or at the very least, its harm mitigated.

11. SHEIN knew, or should have known, that its data security measures were inadequate. SHEIN's Data Breach followed prominent breaches involving other e-commerce websites such as panerabread.com, adidas.com, orbitz.com, macys.com, bloomingsdales.com, and zappos.com.

12. As a result of the Data Breach, Plaintiff's and Class members' Customer Data has been exposed to criminals for misuse. The injuries suffered or that will likely be suffered by Plaintiffs and Class members as a direct result of SHEIN's data breach include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

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

d. damages arising from the inability to use their debit or credit card accounts because their accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the data breach including but not limited to foregoing cash back rewards;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the SHEIN data breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Customer Data being placed in the hands of criminals and already misused via the use of Plaintiff's and Class members' Customer data on the Internet black market, including in illegal "credential stuffing" schemes. This is especially important because SHEIN did not warn Plaintiff and other Class members of the impact of

credential stuffing on their other e-commerce accounts, and failed to recommend that they change their credentials on those platforms as well.

h. damages to and diminution in value of their Customer Data entrusted to SHEIN for the sole purpose of purchasing products from SHEIN and with the mutual understanding that SHEIN would safeguard Plaintiff's and Class members' data against theft and not allow access to and misuse of their information by others;

i. money paid for products purchased at SHEIN during the period of the Data Breach, in that Plaintiff and Class members would not have shopped at SHEIN had SHEIN disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Customer Data; and

j. continued risk to their Customer Data which remains in the possession of SHEIN and which is subject to further breaches so long as SHEIN fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

13. These injuries to the Plaintiff and Class members were directly and proximately caused by SHEIN's failure to implement or maintain adequate data security measures for Customer Data.

14. Plaintiff and Class members retain a significant interest in ensuring that their Customer Data, which remains in SHEIN's possession, is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated customers whose Customer Data was stolen as a result of the SHEIN Data Breach.

15. Plaintiff, on behalf of herself and similarly situated consumers, seeks to recover damages, equitable relief including injunctive relief to prevent a reoccurrence of the data breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs, there are more than 100 putative class members nationwide, and at least one putative class member and SHEIN are citizens of different states.

17. This Court has personal jurisdiction over SHEIN because SHEIN is incorporated, has its headquarters, and conducts substantial business in California, including this District, and has sufficient minimum contacts in California. Accordingly, SHEIN intentionally avails itself of this jurisdiction by marketing, distributing, and selling products throughout California, including this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claims occurred in this District. Specifically, Plaintiff created her SHEIN account by providing her Customer Data to SHEIN in this District. Furthermore, venue is also proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because SHEIN resides in this District.

PARTIES

A. Plaintiff

19. Plaintiff Rosalie Golbahar is a resident of Los Angeles, California and was a California resident during the period of the SHEIN data breach. In or around April 2016, Plaintiff created an account with SHEIN, providing her email address and creating a password for login. Plaintiff used the same email and password login that she had used on certain other online websites. Upon her first purchase in or around April 2016, Plaintiff also provided SHEIN with the credit card information for her American Express card.

20. On or around September 19, 2018, Plaintiff received multiple fraud alert text messages from American Express, notifying her of multiple unauthorized charges

on her American Express credit card, totaling approximately $10,000. Plaintiff's payment card was compromised despite her having physical possession of the payment card at all times.

21. As a result of the fraudulent activity on her card, Plaintiff was forced to call and cancel her American Express card, and was to be issued a new card. Since Plaintiff could no longer use her card, Plaintiff had to drive to her bank on two separate occasions to withdraw cash. The bank was approximately 5 miles away from her home and she spent approximately 20 minutes driving to and from the bank each way. In doing so, Mr. Golbahar expended cash in the form of gasoline expended to get to the bank. Specifically, Mr. Golbahar used approximately .83 gallons of gasoline driving to and from the bank, which cost her approximately $3.16 at the time.

22. As a result of the fraudulent activity on her card, Mr. Golbhar has also expended approximately 20 hours in total so far contacting her banks, updating her payment card information and credentials with various retailers, and reviewing monthly financial statements for any fraudulent or suspicious charges.

23. Plaintiff would not have spent this time and money otherwise had it not been for the Data Breach.

24. From September 19, 2018 until around September 30, 2018, Plaintiff went without her American Express credit card as she was waiting for a replacement card to be issued. As a result, Plaintiff was also forced to use cash or her debit card (which doe not earn cashback) during that time period, and therefore forewent the cashback dollars she would have made by using her American Express credit card. Specifically, her American Express has a cashback of 1% on all purchases. Plaintiff spent approximately $2000 in cash and debit card purchases on necessities, during the period she went without her American Express card. Therefore, Plaintiff forewent approximately $20 in casback dollars.

25. On October 1, 2018, by way of letter, SHEIN notified Plaintiff that her Customer Data was stolen.

26. On or around October 12, 2018, Plaintiff received another fraud alert text message from American Express, notifying her that another attempt to charge her American Express credit card was made.

27. On or around November 13, 2018, an unknown person attempted to make unauthortized charges on Plaintiff's Chase Freedom card.

28. Plaintiff would not have created a SHEIN account or made a purchase with her credit card at SHEIN had SHEIN told her that it lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft.

29. Plaintiff suffered actual injury from having her Customer Data compromised and stolen in and as a result of the SHEIN data breach.

30. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Customer Data – a form of intangible property that she entrusted to SHEIN for the purpose of shopping at SHEIN and that was compromised in and as a result of SHEIN's Data Breach.

31. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her Customer Data being placed in the hands of criminals who have already misused such information stolen in the Data Breach via sale of Plaintiff's and Class members' Customer Data on the internet black market. Plaintiff has a continuing interest in ensuring that her private information, which remains in SHEIN's possession, is protected and safeguarded from future breaches.

32. Plaintiff is likely to continue using the SHEIN website if SHEIN's data security was improved to protect against future data breaches. However, absent an injunction, Plaintiff cannot be certain whether the SHEIN website is safe to use or not.

B. Defendant

33. Defendant SHEIN Fashion Group, Inc. is a corporation organized and existing under the laws of the state of California with its principal place of business located at 345 N. Baldwin Park Boulevard, City of Industry, California 91746. SHEIN distributes and/or sells SHEIN brand garments via its retail website www.us.shein.com throughout the United States, including in this District. SHEIN is an e-commerce fashion retailer dedicated to women's fashion.[8] The company was founded in 2008, and it currently ships to over 230 countries and regions all over the world. Based on information and belief, the data security decisions underlying this action stemmed from SHEIN's presence in California.

STATEMENT OF FACTS

A. Value of Customer Data On the Cyber Black Market

34. Stolen private information is a valuable commodity. A "cyber black-market", exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. The private data is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

35. Legitimate organizations and the criminal underground alike recognize the value in private personal data contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it.

36. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes

[8] https://us.shein.com/About-US-a-117.html (last visited on December 13, 2018)

[9] 17 C.F.R § 248.201 (2013).

"identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[10]

37. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[11]

38. Identity thieves can use personal information, such as that of Plaintiff and Class members which SHEIN failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

39. Highly relevant to this particular Data Breach, hackers can engage in "credential stuffing," a type of cyberattack where stolen account login credentials are used to gain unauthorized access to a user's other online accounts through large-scale automated login requests directed against a web application.[12] This is "a bit like a thief finding a ring of keys in an apartment lobby and trying them, one after the other, in every door in the building. Software makes the trial-and-error process practically instantaneous."[13] This very often result in a "ripple effect" where the hackers gain

[10] *Id.*

[11] Federal Trade Commission, *Warning Signs of Identity Theft, available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited December 13, 2018).

[12] https://www.owasp.org/index.php/Credential_stuffing (last visited on December 13, 2018).

[13] https://www.neweurope.eu/article/password-breach-ripple-effects-well-beyond-yahoo/ (last visited on December 13, 2018).

unauthorized access to other personal data stored on a consumer's other online accounts, such as payment card data, social security numbers, driver license numbers, addresses, and even other account credentials.

40. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[14]

41. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[15]

42. There may be a time lag between when harm occurs versus when it is discovered, and also between when customer data is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [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 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.[16]

---

[14] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited December 13, 2018).

[15] Victims of Identity Theft, 2014 (Sept. 2015) *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited December 13, 2018).

[16] GAO, Report to Congressional Requesters, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited December 13, 2018).

B. SHEIN Had Notice of Data Breaches Involving E-Commerce Websites

43. At all relevant times, SHEIN knew, or reasonably should have known, of the importance of safeguarding the highly sensitive Customer Data 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.

44. In 2017, the number of U.S. data breaches was approximately 1,300, and the 2018 number is expected to surpass this.[17]

45. More specifically, a significant number of the data breaches in the past few years targeted e-commerce websites such as SHEIN, including data breaches affecting panerabread.com, adidas.com, orbitz.com, macys.com, bloomingsdales.com, and zappos.com.

46. SHEIN was aware of the importance of safeguarding customers' sensitive private data as is evident by SHEIN's privacy policy stating and warranting that: "We use reasonable technical, administrative, and physical security measures designed to safeguard and help prevent unauthorized access to your data, and to correctly use the data we collect. For example, access to your personal data is restricted to our employees, contractors, and agents who need access to such data to perform their assigned job duties."[18]

47. However, in this situation, SHEIN was "reactive" rather than "proactive" in protecting against cybersecurity incidents.[19]

48. Unfortunately, and as alleged below, despite all the publicly available knowledge of the continued compromises of customer data, especially in the e-

[17] https://medium.com/@AxelUnlimited/enough-is-enough-2018-has-seen-600-too-many-data-breaches-9e3e5cd8ff78 (last visited December 13, 2018).
[18] https://us.shein.com/Privacy-Security-Policy-a282.html?ref=www&rep=dir&ret=us (last visited December 13, 2018).
[19] https://www.retaildive.com/news/visa-adds-payment-partners-to-network-token-service/539980/ (last visited December 13, 2018).

commerce industry, SHEIN's approach to maintaining the privacy and security of the Plaintiff's and Class members' Consumer Data was lackadaisical, cavalier, reckless, or at the very least, negligent.

C. SHEIN Failed to Comply With FTC Requirements

49. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[21] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

---

[20] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited December 13, 2018).

[21] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136 proteting-personal-information.pdf (last visited December 13, 2018).

51. The FTC also recommends that companies limit access to sensitive data, require complex and secure passwords to be used on networks, require authentication, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[22]

52. Specifically, the FTC has observed that "[c]onsumers and employees often reuse usernames and passwords across different online accounts, making those credentials extremely valuable to remote attackers."[23] As a result, "[c]redentials are sold on the dark web and used to perpetrate credential stuffing attacks – a kind of attack in which hackers automatically, and on a large scale, input stolen usernames and passwords into popular internet sites to determine if any of them work."[24]

53. To combat credential stuffing, the FTC requires companies to "combine multiple authentication techniques," such as strong password requirements, two-factor authentication, and credential screening.[25] [26]

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

---

[22] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited December 13, 2018).

[23] https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication (last visited December 13, 2018).

[24] *Id.*

[25] https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication (last visited December 13, 2018).

[26] https://www.passwordping.com/ftc_credential_stuffing_ato/ (last visited December 13, 2018).

actions further clarify the measures businesses must take to meet their data security obligations.

55. SHEIN's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, including by requiring more complex and unique passwords, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. SHEIN's failure to warn affected consumers about the substantial risk of credential stuffing and to instruct affected consumers to change their credentials on other websites also constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

56. In this case, SHEIN was at all times fully aware of its obligation to protect the private data of its customers. SHEIN was also aware of the significant repercussions if it failed to do so because SHEIN collects private information from millions of customers and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

57. Despite understanding the consequences of inadequate data security, SHEIN failed to comply with FTC requirements and failed to take additional protective measures beyond those required by FTC.

D. The SHEIN Data Breach

58. On August 22, 2018, SHEIN discovered that its customers' email addresses and passwords was stolen by criminals cyberattack, resulting in the unauthorized access of at least 6.42 million users.[27]

59. The Data Breach was active from around June 2018 to early August 2018.[28]

[27] https://www.prnewswire.com/news-releases/shein-notifies-customers-who-may-have-been-affected-by-data-breach-300717103.html (last visited on December 13, 2018).

[28] *Id*.

60. On September 21, 2018, SHEIN announced the Data Breach nearly a month after discovering it, but provided little technical details to customers or the public about how the Data Breach occurred.[29] According to SHEIN, hackers had obtained access to SHEIN customers' Customer Data through "back door" entry points to the SHEIN servers.[30] Since then, despite promises to do so, SHEIN has failed to provide further specific information about how the breach occurred and precisely what information was stolen.

61. Since the Data Breach, SHEIN has also eliminated any reference or notification of the breach from the SHEIN website homepage, perhaps due to the potential negative impact such notice would have on potential shoppers during the holiday season.

62. While SHEIN claims it has not seen evidence that credit card information was stolen in the Data Breach, SHEIN could not definitely disclaim that credit card information was not stolen because SHEIN "***typically*** does not store credit card information on its systems."[31] (emphasis added). Moreover, in its privacy policy, SHEIN claims that "[i]f you make a purchase, we collect personal data in connection with the purchase. This data includes your payment data, such as your credit or debit card number and other card information, and other account and authentication information, as well as billing, shipping, and contact details."[32]

63. Furthermore, with the known Customer Data stolen, criminals can engage in "credential stuffing," a type of cyberattack where stolen account credentials (typically usernames, emails, and passwords) are used to gain unauthorized access to a

---

[29] *Id.*
[30] *Id.*
[31] https://us.shein.com/datasecurity?ref=www&rep=dir&ret=us (last visited December 13, 2018).
[32] https://us.shein.com/Privacy-Security-Policy-a-282.html (last visited on December 13, 2018)

user's other accounts through large-scale automated login requests directed against a web application.[33] It is estimated that credential stuffing bots access 3-8% of the target accounts using compromised credentials from the dark web.[34] As a result of the "ripple effect" of credential stuffing, hackers can obtain a consumer's other personal and sensitive information, including payment card information, social security numbers, driver license numbers, addresses, and other login credentials. This is precisely what happened to Plaintiff.

64. In addition to SHEIN's failure to prevent or detect the Data Breach for about two months, SHEIN chose to remain silent upon discovering the Data Breach, waiting over one month before disclosing the breach to its customers or the public. Plaintiff was not notified of the Data Breach until she received a letter from SHEIN dated October 1, 2018.

65. Had SHEIN implemented and maintained adequate safeguards to protect the Customer Data, deter the hackers, and detect the data breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented and customers would have been able to take earlier action to mitigate their damages.

66. In permitting the Data Breach to occur, SHEIN breached its implied agreement with customers to protect their personal and financial information and violated industry standards.

E. The SHEIN Data Breach Has Caused Harm and Will Result In Future Harm

67. Plaintiff's and Class members' Consumer Data is private and sensitive in nature and was left inadequately protected by SHEIN. SHEIN did not obtain Plaintiff's

[33] https://www.owasp.org/index.php/Credential_stuffing (last visited on December 13, 2018).

[34] https://www.passwordping.com/ftc_credential_stuffing_ato/ last visited on December 13, 2018).

and Class members' consent to disclose their Customer Data to any unauthorized persons as required by applicable law and industry standards.

68. The SHEIN Data Breach was a direct and proximate result of its failure to properly safeguard and protect Plaintiff's and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including SHEIN's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

69. Due to SHEIN's failure to adequately secure the Customer Data and timely identify the breach, the hackers were able to extract sensitive personal data from SHEIN's customers for approximately two months. Customers, including Plaintiff and Class members, have been left exposed, unknowingly and unwittingly, to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

70. As a direct and proximate result of SHEIN's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to expend money and take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it

is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

71. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

72. As a result of the Data Breach, Plaintiff's and Class members' Customer Data has been exposed to criminals for misuse. The injuries suffered or that will likely be suffered by Plaintiffs and Class members as a direct result of SHEIN's data breach include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

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

d. damages arising from the inability to use their debit or credit card accounts because their accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the data breach including but not limited to foregoing cash back rewards;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the SHEIN data breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Customer Data being placed in the hands of criminals and already misused via the use of Plaintiff's and Class members' Customer data on the Internet black market, including in illegal "credential stuffing" schemes. This is especially important because SHEIN did not warn Plaintiff and other Class members of the impact of credential stuffing on their other e-commerce accounts, and failed to recommend that they change their credentials on those platforms as well;

h. damages to and diminution in value of their Customer Data entrusted to SHEIN for the sole purpose of purchasing products SHEIN and with the mutual understanding that SHEIN would safeguard Plaintiff's and Class members' data against theft and not allow access to and misuse of their information by others;

i. money paid for products purchased at SHEIN during the period of the Data Breach, in that Plaintiff and Class members would not have shopped at SHEIN had SHEIN disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Customer Data; and

j. continued risk to their Customer Data which remains in the possession of SHEIN and which is subject to further breaches so long as

SHEIN fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

73. While the Plaintiff's and Class members' Consumer Data has been stolen, SHEIN continues to hold Customer Data of its customers. Particularly because SHEIN has demonstrated an inability to prevent a breach or detect it after running unhindered for approximately two months, Plaintiff and members of the Class have an undeniable interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

74. Plaintiff seeks relief on behalf of herself and as the representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), and (b)(3), Plaintiff seeks to certify a class of all persons residing in the United States whose Customer Data was stolen from SHEIN during the Data Breach (the "Nationwide Class").

75. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff also seeks to certify a class of all persons residing in California whose Customer Data was stolen from SHEIN during the Data Breach (the "California Subclass").

76. The Nationwide Class and California Subclass are individually referred to as "Class" and collectively referred to as the "Classes."

77. Excluded from each of the Classes is SHEIN and any of its parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judges to whom this case is assigned as well as his or her judicial staff and immediate family members.

78. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

79. Plaintiff is a member of both Classes.

80. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3):

81. **Numerosity.** The proposed Classes includes at least 6.42 million customers whose data was compromised in the breach. The massive size of the SHEIN data breach indicates that joinder of each member would be impracticable.

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

a. Whether SHEIN had a duty to protect the Customer Data;

b. Whether SHEIN knew or should have known of the susceptibility of their data security to a data breach;

c. Whether SHEIN's security measures to protect their data were reasonable in light of the FTC data security requirements, and other measures recommended by data security experts;

d. Whether SHEIN was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether SHEIN's failure to implement adequate data security measures allowed the data breach;

f. Whether SHEIN's conduct constituted unfair, unlawful, and/or deceptive trade practices under California law;

g. Whether SHEIN's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Customer Data of Plaintiff and Class members;

h. Whether SHEIN was negligent as a result of its possible violation of relevant statutes, such as Cal. Civ. Code Sections 1798.81.5;

i. Whether SHEIN's breaches of its legal duties caused Plaintiff and the Class members to suffer damages;

j. Whether Plaintiff and Class members are entitled to recover damages; and

k. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

83. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of the claims of the Classes. Plaintiff and Class members were injured through SHEIN's uniform misconduct and their legal claims arise from the same core practices employed or omitted by SHEIN.

84. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiff is an adequate representative of the proposed Classes because her interests do not conflict with the interests of the Class members she seeks to represent. Plaintiff's counsel are experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have successfully prosecuted similarly massive retail data breach cases.

85. **Superiority. Fed. R. Civ. P. 23(a)(5).** 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 SHEIN. Even if it were economically feasible, requiring millions of injured plaintiffs 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.

86. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). SHEIN has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

87. Finally, all members of the proposed Classes are readily ascertainable. SHEIN has access to information regarding which of its stores were affected by the breach, the time period of the breach, which customers were potentially affected, as well as the addresses and other contact information for members of the Classes, which can be used for providing notice to the Class members.

COUNT I
Breach Of Implied Contract
(*On Behalf Of Plaintiff And The Nationwide Class Or, Alternatively, Plaintiff And The California Subclass*)

88. Plaintiff restates and realleges Paragraphs 1 through 87 as if fully set forth herein.

89. SHEIN solicited and invited Plaintiff and Class members to create accounts and provide their Customer Data in order to make purchases on the website. Plaintiff and Class members accepted SHEIN's offer, provided their Customer Data and used their credit or debit cards to make purchases at SHEIN stores during the period of the Data Breach.

90. In so doing, Plaintiff and Class members entered into implied contracts with SHEIN pursuant to which SHEIN agreed to safeguard and protect such information and to timely detect any breaches of their Customer Data.

91. Plaintiff and Class members would not have provided and entrusted their Customer Data to SHEIN in the absence of the implied contract between them and SHEIN.

92. Plaintiffs and Class members fully performed their obligations under the implied contracts with SHEIN.

93. SHEIN's obligations under the implied contracts were to be executed in California, as Plaintiff is a resident of California and she provided her Customer Data to SHEIN in California.

94. SHEIN breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect their Consumer Data and by failing to timely detect the data breach within a reasonable time.

95. As a direct and proximate result of SHEIN's breaches of the implied contracts between SHEIN and Plaintiffs and Class members, Plaintiffs and Class members sustained actual losses and damages as described in detail above.

COUNT II
Negligence
(*On Behalf Of Plaintiff And The Nationwide Class Or, Alternatively, Plaintiff And The California Subclass*)

96. Plaintiff restates and realleges Paragraphs 1 through 87 as if fully set forth herein.

97. Upon accepting and storing the Plaintiff's and Class members' Customer Data in its computer systems and on its networks, SHEIN undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. SHEIN knew that the Customer Data was private and confidential and should be protected as private and confidential.

98. SHEIN owed a duty of care not to subject Plaintiff's and Class members' Customer Data to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

99. SHEIN owed numerous duties to Plaintiff and Class members, including the following:

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

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

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

100. SHEIN breached its duty to Plaintiff and Class members to adequately protect and safeguard Customer Data by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to the Customer Data. Furthering their dilatory practices, SHEIN failed to provide adequate supervision and oversight of the Customer Data with which they were and are entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather the Customer Data of Plaintiff and Class members, misuse the Customer Data and intentionally disclose it to others without consent.

101. SHEIN knew, or should have known, of the risks inherent in collecting and storing Customer Data, the risks of credential stuffing, and the importance of adequate security. SHEIN knew or should have known about numerous, well-publicized data breaches within the retail and e-commerce industry.

102. SHEIN knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' Customer Data.

103. Because SHEIN knew that a breach of its systems would damage millions of its customers, including Plaintiff and Class members, SHEIN had a duty to adequately protect their data systems and the Customer Data contained thereon.

104. SHEIN had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust SHEIN with their Customer Data

was predicated on the understanding that SHEIN would take adequate security precautions. Moreover, only SHEIN had the ability to protect its systems and the Customer Data it stored on them from attack.

105. SHEIN breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Customer Data.

106. SHEIN's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Customer Data. SHEIN's misconduct included failing to: (1) secure its data security systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

107. SHEIN also had independent duties under state and federal laws that required it to reasonably safeguard Plaintiff's and Class members' Customer Data and promptly notify them about the data breach.

108. SHEIN breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Customer Data;

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

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' Customer Data;

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach;

e. by failing to discover the breach for approximately two months; and

f. by failing to alert Plaintiff and Class Members of the substantial risk of credential stuffing and to instruct them to change their login credentials on other e-commerce and web platforms they use.

109. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Customer Data as described in this Complaint.

110. As a direct and proximate cause of SHEIN's conduct, Plaintiff and the Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards; damages arising from Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including, but not limited to, late fees charged and foregone cash back rewards; damages from lost money, time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
Violation Of Cal. Civ. Code § 1798.81.5
(*On Behalf Of Plaintiff And The California Subclass*)

111. Plaintiff restates and realleges paragraphs 1 through 87 above as if fully set forth herein.

112. Cal Civ. Code § 1798.81.5(a)(1) provides that its purpose is to "ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

113. Cal. Civ. Code § 1798.81.5(b) provides, in pertinent part, that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

114. Under Cal Civ. Code § 1798.81.5(d)(1)(B), "personal information" means a "username or email address in combination with a password or security question and answer that would permit access to an online account."

115. Therefore, the Customer Data stolen in the SHEIN Breach, which includes Plaintiff and Class members' email addresses and passwords, falls within the meaning of "personal information" under Cal. Civ. Code Section 1798.81.5.

116. By failing to implement adequate and reasonable data security measures for this Customer Data, SHEIN violated Cal. Civ. Code Section 1798.81.5.

117. Because SHEIN violated Cal. Civ. Code Sections 1798.81.5, Plaintiff may seek an injunction pursuant to Cal. Civ. Code Section 1798.84(e), which states "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined." Specifically, Plaintiff seeks injunctive relief requiring SHEIN to implement and maintain adequate and reasonable data security measures and abide by the California Data Breach laws, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on SHEIN's systems

periodically, and ordering SHEIN to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training its security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of firewalls and access controls so that if one area of SHEIN's data security measures are compromised, hackers cannot gain access to other areas of SHEIN's systems;

f. utilizing more complex and multilayered authentication;

g. requiring consumers use more complex and unique passwords;

h. warning consumers of the substantial risks and effects of credential stuffing, instructing affected consumers to change their credentials on other e-commerce and web platforms they use.

i. deleting, in a reasonable and secure manner, Customer Data not necessary for SHEIN's provisions of products;

j. conducting regular database scanning and security checks;

k. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and contain a breach when it occurs and what appropriate actions are proper in response to a breach; and

l. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

COUNT IV
Negligence *Per Se*
(*On Behalf Of Plaintiff And The Classes*)

On Behalf of the California Subclass

118. Plaintiff restates and realleges Paragraphs 1 through 87 as if fully set forth herein.

119. Section 1798.81.5(b) of the California Civil Code establishes that any "business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

120. SHEIN violated Section 1798.81.5(b) of the California Civil Code by failing to implement and maintain reasonable security procedures and practices necessary to protect Plaintiff and Class members' private information from unauthorized access.

121. SHEIN's violation of Section 1798.81.5(b) of the California Civil Code thereby constitutes negligence *per se*.

122. Plaintiff and Class members are within the class of persons that California Civil Code Section 1798.81.5(b) was intended to protect because they are California residents.

123. The harm which occurred due to SHEIN's Data Breach is the type of harm that California Civil Code Section 1798.81.5(b) was intended to protect. Specifically, this is the harm of the unauthorized access or disclosure of personal information due to a failure to maintain reasonable security procedures.

On Behalf of the Classes

124. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as SHEIN, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form part of the basis of SHEIN's duty in this regard.

125. SHEIN violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards, as described in detail herein. SHEIN's conduct was particularly unreasonable given the nature and amount of Customer Data it obtained and stored, including, specifically, the immense damages that would result to Plaintiff and Class members.

126. SHEIN's violations of Section 5 of the FTC Act constitute negligence *per se*.

127. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

128. The harm that occurred as a result of the SHEIN's Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

129. As a direct and proximate result of SHEIN's negligence *per se*, Plaintiff and the Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards; damages arising from Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including,

but not limited to, late fees charged and foregone cash back rewards; damages from lost money, time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT V
Unjust Enrichment
(*On Behalf Of Plaintiff And The Nationwide Class Or, Alternatively, Plaintiff And The California Subclass*)

130. Plaintiff restates and realleges Paragraphs 1 through 87 as if fully set forth here.

131. Plaintiff and Class members conferred a monetary benefit on SHEIN. Specifically, they purchased goods from SHEIN and provided SHEIN with their Customer Data and payment information. In exchange, Plaintiff and Class members should have received from SHEIN the goods that were the subject of the transaction and should have been entitled to have SHEIN protect their Customer Data with adequate data security.

132. SHEIN knew that Plaintiff and Class members conferred a benefit on it and has accepted or retained that benefit. SHEIN profited from the purchases and used Plaintiff's and Class members' Customer Data for business purposes.

133. SHEIN failed to secure Plaintiff's and Class members' Customer Data and, therefore, did not provide full compensation for the benefit the Plaintiff's and Class members' Customer Data provided.

134. SHEIN acquired the Customer Data through inequitable means as it failed to disclose the inadequate security practices previously alleged.

135. If Plaintiff and Class members knew that SHEIN would not secure their Customer Data using adequate security, they would not have made purchases at SHEIN stores.

136. Plaintiff and Class members have no adequate remedy at law.

137. Under the circumstances, it would be unjust for SHEIN to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

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

COUNT VI
Declaratory Judgment
(*On Behalf Of Plaintiff And The Nationwide Class Or, Alternatively, Plaintiff And The California Subclass*)

139. Plaintiff restates and realleges Paragraphs 1 through 87 as if fully set forth here.

140. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this Complaint.

141. As previously alleged, Plaintiff and Class members entered into an implied contract that required SHEIN to provide adequate security for the Customer

Data it collected from their creating accounts and purchasing goods from the SHEIN website. As previously alleged, SHEIN owes duties of care to Plaintiff and Class members that require it to adequately secure that Customer Data.

142. SHEIN still possesses Customer Data pertaining to Plaintiff and Class members.

143. Accordingly, SHEIN has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that SHEIN's lax approach towards data security has become public, the Customer Data in its possession is more vulnerable than previously.

144. Actual harm has arisen in the wake of the SHEIN Data Breach regarding SHEIN's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

145. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. SHEIN continues to owe a legal duty to secure consumers' Customer Data and to timely and accurately notify consumers of the data breach under California law, common law, and Section 5 of the FTC Act;

b. SHEIN's existing data security measures do not comply with their legal duties of care; and

c. SHEIN continues to breach its legal duty by failing to employ reasonable measures to secure consumers' Customer Data.

146. Plaintiff, also requests an injunction requiring SHEIN to comply with its contractual obligations and duties of care and implement and maintain reasonable security measures, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including

simulated attacks, penetration tests, and audits on SHEIN's systems periodically, and ordering SHEIN to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement[ing] and maintain[ing] reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training its security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of firewalls and access controls so that if one area of SHEIN's data security measures are compromised, hackers cannot gain access to other areas of SHEIN's systems;

f. utilizing more complex and multilayered authentication;

g. requiring consumers use more complex and unique passwords;

h. warning consumers of the substantial risks and effects of credential stuffing, instructing affected consumers to change their credentials on other e-commerce and web platforms they use.

i. deleting, in a reasonable and secure manner, Customer Data not necessary for SHEIN's provisions of goods;

j. conducting regular database scanning and security checks;

k. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and

contain a breach when it occurs and what appropriate actions are proper in response to a breach; and

l. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

147. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event SHEIN incurs another data breach. The risk of another such breach is real, immediate, and substantial.

148. The hardship to Plaintiff and other customers if an injunction is not issued exceeds the hardship to SHEIN if an injunction is issued. If SHEIN incurs another data breach, Plaintiff and other customers will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to SHEIN of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and SHEIN has a pre-existing legal obligation to employ such measures.

149. Such an injunction would benefit the public by preventing another data breach for SHEIN, and therefore eliminating the additional injuries that would result to Plaintiff and the millions of customers whose confidential information would be further compromised.

COUNT VII

Violation Of California's Unfair Competition Law ("UCL"), California Business & Professions Code §§ 17200, *et seq.* (*On Behalf Of Plaintiff And The Nationwide Class Or, Alternatively, Plaintiff And The California Subclass*)

150. Plaintiff restates and realleges Paragraphs 1 through 87 above as if fully set forth herein.

151. UCL § 17200 provides, in pertinent part, that "unfair competition shall mean and include unlawful, unfair, or fraudulent business practices [. . .]".

152. Under the UCL, a business act or practice is "unlawful" if the act or

practice violates any established state or federal law.

153. SHEIN's failures to implement and maintain reasonable security measures and to timely and properly notify Plaintiff and Class members of the Data Breach therefore was and continues to be "unlawful" as SHEIN breached its implied and express warranties and violated the California laws regarding data breaches, including California Civil Code §§ 1798.81.5, as well as the FTC Act.

154. As a result of SHEIN's unlawful business acts and practices, SHEIN unlawfully obtained money from Plaintiff and members of the Class.

155. Under the UCL, a business act or practice is "unfair" if the defendant's conduct is substantially injurious to consumers, goes against public policy, and is immoral, unethical, oppressive, and unscrupulous, as the benefits for committing these acts or practices are outweighed by the severity of the harm to the alleged victims.

156. Here, SHEIN's reckless conduct was and continues to be of no benefit to its customers, as it is both injurious and unlawful to those persons who rely on SHEIN's duties and obligations to maintain and implement reasonable data security measures and to monitor for breaches. Having lax data security measures that has resulted in the disclosure of millions of customers' payment card information provides no benefit to consumers. For these reasons, SHEIN's conduct was and continues to be "unfair" under the UCL.

157. As a result of SHEIN's unfair business acts and practices, SHEIN has unfairly and unlawfully obtained money from Plaintiff and members of the Class.

158. Plaintiff requests that this Court enjoin SHEIN from violating the UCL or violating the UCL in the same way in the future, as discussed herein. Otherwise, Plaintiff and members of the Class may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against SHEIN as follows:

a) For an order certifying the Nationwide Class and the California Subclass under Rule 23 of the Federal Rules of Civil Procedure; naming Plaintiff as representative of all Classes; and naming Plaintiff's attorneys as Class Counsel to represent all Classes;

b) For an order declaring that SHEIN's conduct violates the statutes and laws referenced herein;

c) For an order finding in favor of Plaintiff, and all Classes, on all counts asserted herein;

d) For an order awarding all damages in amounts to be determined by the Court and/or jury;

e) For prejudgment interest on all amounts awarded;

f) For interest on the amount of any and all economic losses, at the prevailing legal rate;

g) For an order of restitution and all other forms of equitable monetary relief;

h) For injunctive relief as pleaded or as the Court may deem proper;

i) For an order awarding Plaintiff and all Classes their reasonable attorneys' fees, expenses and costs of suit, including as provided by statute such as under the Federal Rules of Civil Procedure 23(h); and

j) For any other such relief as the Court deems just and proper.

DEMAND FOR TRIAL BY JURY

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

Dated: December 13, 2018 **FARUQI & FARUQI, LLP**

By: */s/ Benjamin Heikali*
Benjamin Heikali, Bar No. 307466
Joshua Nassir, Bar No. 318344
10866 Wilshire Blvd., Suite 1470
Los Angeles, CA 90024
Telephone: 424.256.2884
Fax: 424.256.2885
E-mail: bheikali@faruqilaw.com
E-mail: jnassir@faruqilaw.com