

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 22-066

**Investigation by LETITIA JAMES,
Attorney General of the State of New York, of**

**SHEIN DISTRIBUTION CORPORATION and
ZOETOP BUSINESS COMPANY, LIMITED,**

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to Executive Law § 63(12) and General Business Law (“GBL”) §§ 349 and 899-aa into a data breach involving Zoetop Business Company, Limited (“Zoetop”) and the company’s response to the data breach.¹ This Assurance of Discontinuance (“Assurance”) contains the findings of the NYAG’s investigation and the relief agreed to by the NYAG and Respondents SHEIN Distribution Corporation and Zoetop (“Respondents”), whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the “Parties”).

NYAG FINDINGS

1. During the period covered by this Assurance, Zoetop was an international online

¹ Respondents have represented to the NYAG that, as a result of a corporate restructuring, Zoetop is no longer operational and U.S. operations for the brands involved in the data breach that is the subject of this Assurance – SHEIN and ROMWE – have been taken over by SHEIN Distribution Corporation. Accordingly, both SHEIN Distribution Corporation and Zoetop are the Respondents and signatories to this Assurance. The NYAG will refer to Zoetop in its findings where appropriate.

retailer that operated several websites, including ROMWE.com and SHEIN.com, and mobile apps through which it sold clothing and accessories.

2. Like most retail websites, the ROMWE and SHEIN websites allow customers to create online accounts by entering an email address and choosing a password.

The 2018 Data Breach

3. In June 2018, Zoetop was targeted in a cyberattack. On or about July 18, 2018, Zoetop's payment processor alerted Zoetop that the retailer's systems appeared to have been compromised. The payment processor reported that it had been contacted by a large credit card network and a credit card issuing bank, each of which had information "indicating that [Zoetop's] system[s] have been infiltrated and card data stolen." The credit card network had found some SHEIN customers' credit card numbers for sale on an internet forum known for frequenting in stolen payment card data. Separately, the issuing bank had issued a fraud alert known as a common point of purchase (CPP) report for SHEIN after linking fraud on several of its customers' accounts back to earlier purchases the customers had made with SHEIN. The payment processor required that Zoetop engage a Payment Card Industry ("PCI") approved Forensic Investigator ("PFI") to conduct a PCI investigation.

4. Zoetop, in addition to retaining the PFI, also engaged a cybersecurity firm to conduct a forensic investigation. The cybersecurity firm confirmed that attackers had gained access to certain of Zoetop's systems and had conducted extensive operations on Zoetop's internal network.

5. At the time, Zoetop stored only partial card data (the first 6 and last 4 digits). The cybersecurity firm found evidence that, among other activities, the attackers had altered some

Zoetop code responsible for processing customer transactions in an attempt to intercept and exfiltrate customer credit card information. Thus, any exfiltration of payment card data would have happened by intercepting card data at the point of purchase. The cybersecurity firm was unable to determine whether the credit card information had successfully been exfiltrated.

6. In addition, the cybersecurity firm found that attackers had accessed and likely exfiltrated the personal information of millions of SHEIN account holders, including names, city/province information, email addresses, and hashed account passwords. The firm found that the stolen login credentials (email addresses and hashed passwords) had then been offered for sale on a hacking forum on the Internet. Worldwide, more than 39 million SHEIN account credentials were included in the data exposed online, including the credentials of more than 375,000 New York residents.

7. Although the stolen passwords were hashed, the method Zoetop had used to hash the passwords left them susceptible to password cracking attacks, through which attackers could identify the original, unhashed password. Zoetop had hashed passwords using the MD-5 algorithm, which was known at the time to be an insecure algorithm for hashing passwords. Zoetop had also used a salt that was only two digits which was too short to adequately protect against cracking. Zoetop began phasing out the MD-5 based hashing methodology in August 2018, replacing customers' hashed passwords with passwords protected by a more secure algorithm as they logged into the website. By July 2019, all SHEIN and ROMWE user passwords had been salted and hashed using a more secure algorithm.

8. At the conclusion of Zoetop's investigation in September 2018, Zoetop did not force a password reset for any of the over 39 million SHEIN accounts worldwide whose login

credentials had been stolen in the breach. Instead, Zoetop identified a subset of the more than 39 million impacted accounts that had previously placed an order with SHEIN—6.42 million accounts worldwide, including more than 375,000 New Yorkers—and, of this subset, contacted accounts in the U.S., Canada, and Europe, recommending that these account holders themselves initiate a password reset. Zoetop also offered the U.S. residents in this group identity theft protection at no charge. The bulk of the SHEIN accounts impacted in the breach—more than 32.5 million accounts worldwide, including 255,294 New York residents—were not contacted.

9. Around this time, Zoetop also publicly disclosed the breach, issuing a press release and posting a “Frequently Asked Questions” (“FAQ”) page on its website concerning the breach. Several of the statements the company made in these documents, however, were misleading.

10. In the press release and FAQ, Zoetop stated that approximately 6.42 million customers had been impacted in the breach. The press release also stated that the company was in the process of notifying “customers who may have been affected.”

11. However, as noted above, Zoetop had determined that credentials from more than 39 million accounts had been stolen in the attack. The figure in the press release and on the SHEIN website—6.42 million—included only those accounts that had placed an order with SHEIN. Moreover, contrary to Zoetop’s statement, most accounts affected by the attack were not directly contacted by the company. As noted above, only accounts in the U.S., Canada, and Europe who had placed an order with SHEIN were contacted.

12. Zoetop also made a misrepresentation in the FAQ page posted on the SHEIN website. The FAQ contained the following statement:

Was my credit card information stolen?

We have seen no evidence that your credit card information was taken from

our systems and SHEIN typically does not store credit card information on its systems.²

13. As described above, however, Zoetop was aware of reports conveyed to it by its payment processor that a major credit card network and a credit card issuer had reason to believe “that [Zoetop’s] system ha[s] been infiltrated and card data stolen.”

14. Zoetop’s press release and the letters it sent to customers similarly failed to disclose that customers’ credit card information may have been stolen.

Zoetop’s PCI Forensic Investigation

15. The payment card industry requires merchants that process, store, or transmit cardholder data to adhere to a self-regulatory data security standard known as PCI DSS (Payment Card Industry Data Security Standard). In addition, following a data security incident, merchants are often required to engage a PCI-qualified forensic investigator (PFI) to conduct an investigation into the incident.

16. Pursuant to these rules, Zoetop was required to engage a PFI to conduct a PCI forensic investigation. The PFI was not able to conduct a comprehensive investigation, however, as Zoetop did not provide the firm access to the compromised systems and a variety of information about Zoetop’s data security program. During the PFI’s engagement with Zoetop and prior to acquiring evidence from the environment, several changes had been made to remediate the environment. The PFI was not permitted access to any backups prior to the changes being implemented or any evidence originally acquired by the cybersecurity firm. Nevertheless, in the

² This statement was followed by, “If you believe your credit card information may have been compromised, we urge you to contact your bank or credit card company with any concerns. If you have information to share with us about a problem, we encourage you to reach out to [phone number omitted].”

limited review it conducted, the PFI found several areas in which Zoetop's systems were not compliant with PCI DSS.

17. Notably, the PFI found that Zoetop had failed to adhere to PCI DSS requirements for protecting stored credit card data. The PFI discovered that, although Zoetop generally did not store full payment card numbers, when an error occurred during a transaction, unencrypted credit card information was saved to a debug log file. These debug log files contained credit card information from 27,295 transactions that took place between December 2016 and August 2018, a small subset of the credit card transactions that took place during that time period. The firm was unable to determine whether attackers had exfiltrated the log files.

18. The PFI also found that, at the time of the incident, Zoetop failed to adhere to PCI DSS requirements related to network monitoring and testing, as the company did not use file integrity monitoring, monitor or analyze log files, retain an audit trail history, or perform quarterly network vulnerability scans.

19. Finally, the PFI found that Zoetop either had not developed, implemented and documented a variety of policies and procedures as required by PCI DSS, or had simply refused to provide the forensic firm with copies of the documented policies and procedures, including a data security policy, an incident response plan, and policies and procedures for protecting stored cardholder data, developing and maintaining secured systems and applications, monitoring access to network resources and cardholder data, and log retention.

20. Zoetop became independently certified as PCI DSS compliant in April 2019 and has remained so since.

The 2020 Discovery of Stolen ROWME Credentials

21. On June 12, 2020, Zoetop discovered that customer login credentials for another website it operated, ROMWE.com, were available on the dark web. Unlike the SHEIN credentials found in 2018, the ROMWE credentials were in plaintext.

22. Zoetop engaged a cybersecurity firm to investigate. Based on the results of the investigation, Zoetop concluded that the ROMWE login credentials had likely been exfiltrated in 2018 in the same attack that had impacted SHEIN accounts. Zoetop also concluded that the passwords had likely been hashed at the time of exfiltration and were in plaintext at the time of discovery because they had subsequently been cracked. As noted above, the algorithm that Zoetop used to hash passwords in 2018 was susceptible to cracking.

23. On or about June 18, 2020, Zoetop reset the passwords of affected ROMWE customer accounts. Zoetop did not at that time contact these customers to inform them that their login credentials had been exfiltrated and exposed online, or that their passwords had been reset as a result. Instead, Zoetop presented impacted customers who attempted to log in to their ROMWE accounts with a password reset message prompt. From June 2020 to September 2020, the message prompt read as follows: “Your password has a low security level and may be at risk. Please change your login password.”

24. In light of its finding that hashed passwords to ROMWE accounts had likely been cracked, Zoetop revisited its 2018 response to the theft of SHEIN account credentials. In September 2020, Zoetop began forcing password resets for all SHEIN accounts impacted in the 2018 breach that had not previously been reset.

25. Although Zoetop reset the passwords to these SHEIN accounts, Zoetop did not

contact these customers to inform them that their login credentials had been stolen in 2018 or that their passwords had been reset as a result. Instead, Zoetop presented impacted customers logging in to their SHEIN accounts with the following inaccurate message: “Your password has not been updated in more than 365 days. For your protection, please update it now.” This message was shown to SHEIN customers until June 8, 2021, after which the message was updated to state: “We detected suspicious activity, please verify your identity in order to restore your account.”

26. On December 11 and 12, 2020, Zoetop discovered that additional login credentials for ROMWE customer accounts had been discovered on the dark web. On December 14, Zoetop reset the passwords for all ROMWE customer accounts that existed at the time of the 2018 security incident and that had not previously been reset.

27. Following the password reset, ROMWE customers who attempted to log in to their accounts were presented with the following inaccurate message: “Your password has not been updated in more than 365 days. For your protection, please update it now.” This message was shown to ROMWE customers until February 10, 2021, after which time it was replaced with the following: “We detected suspicious activity, please verify your identity in order to restore your account.”

28. On December 30, 2020, Zoetop began emailing ROMWE customers to notify them of the security incident. Impacted U.S. customers were offered identity theft protection services at no charge. Zoetop also posted a notice entitled “ROMWE Notifies Customers of Data Security Incident” and a set of FAQs regarding the incident on the ROMWE website, established a toll-free call center to answer customers’ questions about the incident, and issued a press release.

29. In all, the login credentials of nearly 7.3 million ROMWE accounts, including

nearly 500,000 New York residents, were stolen in the 2018 breach.

Zoetop's Representations Regarding Data Security

30. Since April 26, 2018, the online privacy policies for the ROMWE and SHEIN websites have contained the following representation to consumers:

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.

31. Despite this representation, Zoetop failed to maintain reasonable security measures to protect customers' data in several areas prior to the cyberattack in 2018. These included:

- a. Password Management: Until August 2018, Zoetop hashed customer passwords using the MD-5 algorithm and a two-digit salt. It was known at the time that this method was insufficient to protect against password cracking attacks.
- b. Protection of Sensitive Customer Information: Zoetop misconfigured one of its systems such that unencrypted credit card information from 27,295 transactions that took place between December 2016 and August 2018 were stored in debug log files. In addition, at the time of the breach, Zoetop failed to perform scans to identify where on its systems cardholder data was stored.
- c. Monitoring: At that time, Zoetop did not run regular external vulnerability scans, use file integrity monitoring to detect unauthorized modifications to critical system files, retain an audit trail of a variety of systems, or regularly monitor or review audit logs to identify security incidents.
- d. Incident Response: Zoetop did not have a comprehensive, written incident response plan. In addition, following the 2018 data breach, Zoetop failed to take timely action

to protect many of the impacted customers, such as by alerting customers that their login credentials had been stolen and resetting the passwords of impacted accounts.

Post-Breach Improvements

32. Respondents have represented to the NYAG that they have taken the following steps to improve their information security program since the 2018 breach: implementing a credential stuffing email blocklist that, upon detecting a fraudulent login attempt, requires two-factor email authentication and a password reset to regain access to the account; upgrading its password hashing algorithm; creating alarm triggers that detect suspicious behavior; implementing machine recognition technology that improves the Respondents' ability to distinguish automated or "bot" logins from authentic logins; hiring experienced privacy and data security senior executives and managers; and increasing use of and coordination with third-party cybersecurity and fraud prevention detection vendors.

Respondent Zoetop's Violations

33. Zoetop's conduct violated Executive Law § 63(12), which prohibits repeated fraudulent or illegal acts, GBL § 349, which prohibits deceptive acts and practices, and GBL § 899-aa, which requires disclosure of a data breach to impacted consumers in the most expedient time possible and without unreasonable delay.

34. Respondents neither admit nor deny the NYAG's Findings, paragraphs 1-33 above.

35. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL §§ 349 and 899-aa.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

PROSPECTIVE RELIEF

36. For the purposes of this Assurance, the following definitions shall apply:
- a. “Customer” shall mean any individual whom Respondents can reasonably identify as residing in New York and who provides or has provided Personal Information to Respondents through Respondents’ websites or apps, or in connection with a purchase from Respondents.
 - b. “Personal Information” shall mean information that identifies or relates to an individual, including name, home or other physical address, email address, phone number, account username, account password, Social Security number, government ID number including driver's license number, bank account number, and credit or debit card number.
 - c. “Security Event” shall mean unauthorized access to or acquisition of Personal Information owned, licensed, or maintained by Respondents.

GENERAL COMPLIANCE

37. Respondents shall comply with Executive Law § 63(12) and GBL § 349 in connection with its collection, use, and maintenance of Customer Personal Information, and shall not misrepresent (a) the manner or extent to which it protects the privacy, security, or confidentiality of Personal Information, (b) any aspect of a Security Event, including the Customers and Customer Personal Information impacted, or (c) the basis for resetting a password associated with a Customer account.

INFORMATION SECURITY PROGRAM

38. Respondents shall maintain a comprehensive information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Customer Personal Information that Respondents collect, store, transmit, and/or maintain. Respondents shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include the following processes:

- a. Assess and document, not less than annually, internal and external risks to the security, integrity and confidentiality of Customer Personal Information;
- b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondents identified that are appropriate to: (i) the size and complexity of Respondents’ operations; (ii) the nature and scope of Respondents’ activities; and (iii) the volume and sensitivity of the Customer Personal Information that Respondents collect, store, transmit, and/or maintain.
- c. Assess, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks Respondents identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with (b) above;
- d. Test and monitor the effectiveness of the safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with (b) above;
- e. Select service providers capable of appropriately safeguarding Customer

Personal Information, contractually require service providers to implement and maintain appropriate safeguards to protect Customer Personal Information, and take appropriate steps to verify service providers are complying with the contractual requirements;

- f. Evaluate the Information Security Program not less than annually and adjust the Program in light of any changes to Respondents' operations or business arrangements, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Program.

39. Respondents shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program. The appointed individual shall report at a minimum semi-annually to the Chief Executive Officer and senior management concerning Respondents' security posture, the security risks faced by Respondents, and the Information Security Program.

40. Respondents shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within sixty (60) days of the effective date of this Assurance, or within thirty (30) days of when an employee first assumes responsibility for implementing, maintaining, or monitoring the Information Security Program.

PERSONAL INFORMATION SAFEGUARDS AND CONTROLS

41. Customer Password Management: Respondents shall, to the extent they have not already done so, establish, and, thereafter, maintain appropriate password policies and procedures for Customer accounts. Such policies and procedures shall include strong password requirements and safeguards to protect stored passwords from unauthorized access, including, without limitation, hashing stored passwords using a hashing algorithm and salting policy at a minimum commensurate with NIST standards and security risks that are known or reasonably should be known.

42. Logging & Monitoring: Respondents shall, to the extent they have not already done so, establish, and, thereafter, maintain a system designed to collect and monitor network activity, such as through the use of security and event management tools, as well as policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (1) provide for centralized logging and monitoring that includes collection and aggregation of logging for Respondents' network, and (2) monitor for and alert security personnel to suspicious activity. Logs for network activity should be actively accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

43. Network Vulnerability Scanning: Respondents shall regularly run comprehensive internal and external vulnerability scans of its network not less than quarterly. Scans shall be performed by qualified employees or vendors.

44. Incident Response: Respondents shall, to the extent they have not already done so, establish, and, thereafter, maintain a comprehensive incident response plan. The incident response plan shall be documented in writing and include, at a minimum, the following policies:

- a. If Respondents have reason to believe a Security Event has occurred, Respondents shall promptly conduct a reasonable investigation to determine, at a minimum, whether Customer Personal Information was accessed or acquired without authorization, and, if so, what Customer Personal Information was accessed or acquired.
- b. If Respondents determine Customer Personal Information has been, or is reasonably likely to have been, accessed or acquired without authorization, Respondents shall expediently provide each Customer whose Personal Information has been, or is reasonably believed to have been, accessed or acquired without authorization, by email or letter or other legally valid forms of substitute notice established under New York law, material information concerning the Security Event that is reasonably individualized to the customer including, at a minimum, the timing of the Security Event, whether the Customer's Personal Information was accessed or acquired without authorization, what Personal Information was accessed or acquired, and what actions have been taken to protect the Customer. If necessary in order to provide expedient notice to Customers whose Personal Information has been, or is reasonably believed to have been, accessed or acquired without authorization, Respondents may provide more than one notice that collectively provide all material information.
- c. If Respondents determine that login credentials for Customer accounts have been, or are reasonably likely to have been, accessed or acquired without

authorization, or that Customer accounts have been accessed or acquired without authorization, Respondents shall promptly reset the passwords of those Customer accounts.

INFORMATION SECURITY PROGRAM ASSESSMENTS

45. For a period of five (5) years from the Effective Date, Respondents shall provide to the NYAG copies of the following within two weeks of completion:

- a. Any third-party assessments of Respondents' systems, networks, and/or policies concerning information security; and
- b. Any assessments, questionnaires, scans, procedures, tests, evaluations, and documentation pertaining to Respondents' PCI compliance.

CREDIT MONITORING

46. Respondent shall offer identity theft protection services to all Customers who made a purchase through Respondent prior to the 2018 Security Event, were impacted in the 2018 Security Event, and were not previously offered identity theft protection services.

MONETARY RELIEF

47. Respondents shall collectively pay to the State of New York 1.9 million dollars (\$1,900,000) in penalties and costs. Payment shall be made payable to the State of New York in full within fourteen (14) days of the effective date of this Assurance. Any payment shall reference AOD No. 22-066.

MISCELLANEOUS

48. Respondents expressly agree and acknowledge that NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of

the Assurance, or if the Assurance is voided pursuant to paragraph 55, and agrees and acknowledges that in the event the Assurance is voided pursuant to paragraph 55:

- a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;
- b. the NYAG may use statements, documents or other materials produced or provided by Respondents prior to or after the effective date of this Assurance;
- c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondents irrevocably and unconditionally waive any objection based upon personal jurisdiction, inconvenient forum, or venue; and
- d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

49. If a court of competent jurisdiction determines that Respondents have violated the Assurance, Respondents shall pay to the NYAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

50. This Assurance is not intended for use by any third party in any other proceeding.

51. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondents. Respondents shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of NYAG.

52. Nothing contained herein shall be construed as to deprive any person of any private

right under the law.

53. Any failure by the NYAG to insist upon the strict performance by Respondents of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Respondents.

54. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 22-066, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondents, to:

General Counsel
SHEIN Distribution Corporation
757 South Alameda Street, Suite 340
Los Angeles, CA 90021
Us_legal@sheingroup.com

If to NYAG, to:

Hanna Baek, Assistant Attorney General, or in her absence,
to the person holding the title of Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

55. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondents and its counsel and NYAG's own factual investigation as set forth in NYAG's Findings, paragraphs 1-33 above. Respondents represent and

warrant that neither they nor their counsel have made any material representations to NYAG that are inaccurate or misleading. If any material representations by Respondents or their counsel are later found to be inaccurate or misleading, this Assurance is voidable by NYAG in its sole discretion.

56. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondents in agreeing to this Assurance.

57. Respondents represent and warrant, through the signature below, that the terms and conditions of this Assurance are duly approved.

58. The obligations of this Assurance set forth in ¶¶ 38-44 shall expire at the conclusion of the seven (7) year period after the Effective Date. Provided, however, that nothing in this paragraph shall be construed as excusing or exempting Respondents from complying with any applicable state or federal law or regulation or other applicable law.

59. Respondents agree not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects Respondents' right to take legal or factual positions in defense of litigation or other legal proceedings to which the NYAG is not a party.

60. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that Respondents violate the Assurance after its effective date.

61. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

62. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.



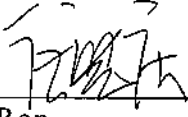
63. Respondents acknowledge that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

64. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

65. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

66. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

67. The effective date of this Assurance shall be the date the NYAG signs the Assurance ("Effective Date").

<p>LETITIA JAMES ATTORNEY GENERAL OF THE STATE OF NEW YORK</p> <p>By:  Hanna Baek Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005 Phone: (212) 416-8433 Fax: (212) 416-8369</p> <p><u>10/12/22</u> Date</p>	<p>SHEIN DISTRIBUTION CORPORATION</p> <p>DocuSigned by: By:  Valerie Ho General Counsel & Corporate Secretary</p> <p>October 5, 2022 Date</p> <p>ZOETOP BUSINESS COMPANY, LIMITED</p> <p>By:  Tony Ren Director</p> <p>October 5, 2022 Date</p>
---	--