OFFICE OF THE ATTORNEY GENERAL
STATE OF FLORIDA
DEPARTMENT OF LEGAL AFFAIRS

CONSUMER PROTECTION
SUBPOENA DUCES TECUM

IN THE INVESTIGATION OF: **Shein US Services, LLC**
AG CASE NO: L25-3-1107

TO: **Shein US Services, LLC**
Paracorp Incorporated
2140 S. Dupont Hwy
Camden, DE 19934
(Or Such Other Address as Service Can be Made)

THIS INVESTIGATIVE SUBPOENA DUCES TECUM is issued pursuant to the Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes, and the Florida Digital Bill of Rights, Chapter 501, Part V, Florida Statutes in the course and authority of an official investigation. Your attention is directed to Sections 501.204, and 501.206, Florida Statutes (2025), printed and attached hereto.

YOU ARE HEREBY COMMANDED to produce all documentary material and other tangible evidence as described herein, that is in your possession, custody, or control, or in the possession, custody, or control of your agents or employees, and to make it available for inspection and copying or reproduction before Bureau Chief - Assistant Attorney General Mandy Mills or Financial Investigator Scott Steitz on **February 26, 2026, at 9:00 a.m.** at the following location:

OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION
110 SE 6th Street, 10th Floor
Fort Lauderdale, FL 33301

ALTERNATIVELY, this subpoena may be complied with by delivering copies of all of the requested materials, prior to the date set forth above, to Bureau Chief - Assistant Attorney General Mandy Mills at Mandy.Mills@myfloridalegal.com and Financial Investigator Scott Steitz at

Scott.Steitz@myfloridalegal.com. The production of material in response to this demand shall include the following:

SEE ATTACHED ADDENDUM

WITNESS, the Department of Legal Affairs at Fort Lauderdale, Florida, this 5th day of February 2026.

JAMES UTHMEIER
ATTORNEY GENERAL

/s/ Mandy L. Mills
Mandy L. Mills, Esq.
Bureau Chief - Assistant Attorney General
Florida Bar No. 41654
Office of the Attorney General
Consumer Protection Division
110 SE 6th Street, 10th Floor
Fort Lauderdale, FL, 33301
Telephone: (954) 712-4600
Mandy.Mills@myfloridalegal.com

501.204 Unlawful acts and practices.—
(1) Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.
(2) It is the intent of the Legislature that, in construing subsection (1), due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to s. 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. s. 45(a)(1) as of July 1, 2017.

501.206 Investigative powers of enforcing authority.—
(1) If, by his or her own inquiry or as a result of complaints, the enforcing authority has reason to believe that a person has engaged in, or is engaging in, an act or practice that violates this part, he or she may administer oaths and affirmations, subpoena witnesses or matter, and collect evidence. Within 5 days, excluding weekends and legal holidays, after the service of a subpoena or at any time before the return date specified therein, whichever is longer, the party served may file in the circuit court in the county in which he or she resides or in which he or she transacts business and serve upon the enforcing authority a petition for an order modifying or setting aside the subpoena. The petitioner may raise any objection or privilege which would be available under this chapter or upon service of such subpoena in a civil action. The subpoena shall inform the party served of his or her rights under this subsection.
(2) If matter that the enforcing authority seeks to obtain by subpoena is located outside the state, the person subpoenaed may make it available to the enforcing authority or his or her representative to examine the matter at the place where it is located. The enforcing authority may designate representatives, including officials of the state in which the matter is located, to inspect the matter on his or her behalf, and he or she may respond to similar requests from officials of other states.
(3) Upon failure of a person without lawful excuse to obey a subpoena and upon reasonable notice to all persons affected, the enforcing authority may apply to the circuit court for an order compelling compliance.
(4) The enforcing authority may request that an individual who refuses to comply with a subpoena on the ground that testimony or matter may incriminate him or her be ordered by the court to provide the testimony or matter. Except in a prosecution for perjury, an individual who complies with a court order to provide testimony or matter after asserting a privilege against self-incrimination to which he or she is entitled by law shall not have the testimony or matter so provided, or evidence derived therefrom, received against him or her in any criminal investigation or proceeding.
(5) Any person upon whom a subpoena is served pursuant to this section shall comply with the terms thereof unless otherwise provided by order of the court. Any person who fails to appear with the intent to avoid, evade, or prevent compliance in whole or in part with any investigation under this part or who removes from any place, conceals, withholds, mutilates, alters, or destroys, or by any other means falsifies any documentary material in the possession, custody, or control of any person subject to any such subpoena, or knowingly conceals any relevant information with the intent to avoid, evade, or prevent compliance shall be liable for a civil penalty of not more than $5,000, reasonable attorney's fees, and costs.

501.702 Definitions.—As used in this part, the term:
(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or that shares common branding with another

legal entity. For purposes of this subsection, the term "control" or "controlled" means any of the following:

(a) The ownership of, or power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company.

(b) The control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(c) The power to exercise controlling influence over the management of a company.

(2) "Aggregate consumer information" means information that relates to a group or category of consumers from which the identity of an individual consumer has been removed and is not reasonably capable of being directly or indirectly associated or linked with any consumer, household, or device. The term does not include information about a group or category of consumers used to facilitate targeted advertising or the display of ads online. The term does not include personal information that has been deidentified.

(3) "Authenticate" or "authenticated" means to verify or the state of having been verified, respectively, through reasonable means that the consumer who is entitled to exercise the consumer's rights under s. 501.705 is the same consumer exercising those consumer rights with respect to the personal data at issue.

(4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs; video or audio recordings or data generated from video or audio recordings; or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(5) "Business associate" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(6) "Child" means an individual younger than 18 years of age.

(7) "Consent," when referring to a consumer, means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative act. The term does not include any of the following:

(a) Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information.

(b) Hovering over, muting, pausing, or closing a given piece of content.

(c) Agreement obtained through the use of dark patterns.

(8) "Consumer" means an individual who is a resident of or is domiciled in this state acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context.

(9) "Controller" means:

(a) A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:

1. Is organized or operated for the profit or financial benefit of its shareholders or owners;

2. Conducts business in this state;

3. Collects personal data about consumers, or is the entity on behalf of which such information is collected;
4. Determines the purposes and means of processing personal data about consumers alone or jointly with others;
5. Makes in excess of $1 billion in global gross annual revenues; and
6. Satisfies at least one of the following:
a. Derives 50 percent or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online;
b. Operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation. For purposes of this sub-subparagraph, a consumer smart speaker and voice command component service does not include a motor vehicle or speaker or device associated with or connected to a vehicle which is operated by a motor vehicle manufacturer or a subsidiary or affiliate thereof; or
c. Operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.
(b) Any entity that controls or is controlled by a controller. As used in this paragraph, the term "control" means:
1. Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller;
2. Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
3. The power to exercise a controlling influence over the management of a company.
(10) "Covered entity" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.
(11) "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. The term includes any practice the Federal Trade Commission refers to as a dark pattern.
(12) "Decision that produces a legal or similarly significant effect concerning a consumer" means a decision made by a controller which results in the provision or denial by the controller of any of the following:
(a) Financial and lending services.
(b) Housing, insurance, or health care services.
(c) Education enrollment.
(d) Employment opportunities.
(e) Criminal justice.
(f) Access to basic necessities, such as food and water.
(13) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual.
(14) "Health care provider" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.
(15) "Health record" means any written, printed, or electronically recorded material maintained by a health care provider in the course of providing health care services to an individual which concerns the individual and the services provided. The term includes any of the following:
(a) The substance of any communication made by an individual to a health care provider in confidence during or in connection with the provision of health care services.
(b) Information otherwise acquired by the health care provider about an individual in

confidence and in connection with health care services provided to the individual.

(16) "Identified or identifiable individual" means a consumer who can be readily identified, directly or indirectly.

(17) "Known child" means a child under circumstances of which a controller has actual knowledge of, or willfully disregards, the child's age.

(18) "Nonprofit organization" means any of the following:

(a) An organization exempt from federal taxation under s. 501(a) of the Internal Revenue Code of 1986 by virtue of being listed as an exempt organization under s. 501(c)(3), s. 501(c)(4), s. 501(c)(6), or s. 501(c)(12) of that code.

(b) A political organization.

(19) "Personal data" means any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

(20) "Political organization" means a party, a committee, an association, a fund, or any other organization, regardless of whether incorporated, organized and operated primarily for the purpose of influencing or attempting to influence any of the following:

(a) The selection, nomination, election, or appointment of an individual to a federal, state, or local public office or an office in a political organization, regardless of whether the individual is selected, nominated, elected, or appointed.

(b) The election of a presidential or vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed.

(21) "Postsecondary education institution" means a Florida College System institution, state university, or nonpublic postsecondary education institution that receives state funds.

(22) "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, which directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. The term does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility.

(23) "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(24) "Processor" means a person who processes personal data on behalf of a controller.

(25) "Profiling" means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(26) "Protected health information" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(27) "Pseudonymous data" means any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the

personal data is not attributed to an identified or identifiable individual.

(28) "Publicly available information" means information lawfully made available through government records, or information that a business has a reasonable basis for believing is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

(29) "Sale of personal data" means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include any of the following:

(a) The disclosure of personal data to a processor who processes the personal data on the controller's behalf.

(b) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer.

(c) The disclosure of information that the consumer:

1. Intentionally made available to the general public through a mass media channel; and

2. Did not restrict to a specific audience.

(d) The disclosure or transfer of personal data to a third party as an asset that is part of a merger or an acquisition.

(30) "Search engine" means technology and systems that use algorithms to sift through and index vast third-party websites and content on the Internet in response to search queries entered by a user. The term does not include the license of search functionality for the purpose of enabling the licensee to operate a third-party search engine service in circumstances where the licensee does not have legal or operational control of the search algorithm, the index from which results are generated, or the ranking order in which the results are provided.

(31) "Sensitive data" means a category of personal data which includes any of the following:

(a) Personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.

(b) Genetic or biometric data processed for the purpose of uniquely identifying an individual.

(c) Personal data collected from a known child.

(d) Precise geolocation data.

(32) "State agency" means any department, commission, board, office, council, authority, or other agency in the executive branch of state government created by the State Constitution or state law. The term includes a postsecondary education institution.

(33) "Targeted advertising" means displaying to a consumer an advertisement selected based on personal data obtained from that consumer's activities over time across affiliated or unaffiliated websites and online applications used to predict the consumer's preferences or interests. The term does not include an advertisement that is:

(a) Based on the context of a consumer's current search query on the controller's own website or online application; or

(b) Directed to a consumer search query on the controller's own website or online application in response to the consumer's request for information or feedback.

(34) "Third party" means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor.

(35) "Trade secret" has the same meaning as in s. 812.081.

(36) "Voice recognition feature" means the function of a device which enables the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds.

501.705 Consumer rights.—
(1) A consumer is entitled to exercise the consumer rights authorized by this section at any time by submitting a request to a controller which specifies the consumer rights that the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise these rights on behalf of the child.
(2) A controller shall comply with an authenticated consumer request to exercise any of the following rights:
(a) To confirm whether a controller is processing the consumer's personal data and to access the personal data.
(b) To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.
(c) To delete any or all personal data provided by or obtained about the consumer.
(d) To obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format.
(e) To opt out of the processing of the personal data for purposes of:
1. Targeted advertising;
2. The sale of personal data; or
3. Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer.
(f) To opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data.
(g) To opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.
(3) A device that has a voice recognition feature, a facial recognition feature, a video recording feature, an audio recording feature, or any other electronic, visual, thermal, or olfactory feature that collects data may not use those features for the purpose of surveillance by the controller, processor, or affiliate of a controller or processor when such features are not in active use by the consumer, unless otherwise expressly authorized by the consumer.

501.71 Controller duties.—
(1) A controller shall:
(a) Limit the collection of personal data to data that is adequate, relevant, and reasonably necessary in relation to the purposes for which it is processed, as disclosed to the consumer; and
(b) For purposes of protecting the confidentiality, integrity, and accessibility of personal data, establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue.
(2) A controller may not do any of the following:
(a) Except as otherwise provided by this part, process personal data for a purpose that is neither reasonably necessary nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.
(b) Process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.
(c) Discriminate against a consumer for exercising any of the consumer rights contained in this part, including by denying goods or services, charging different prices or rates for goods or services, or providing a

different level of quality of goods or services to the consumer. A controller may offer financial incentives, including payments to consumers as compensation, for processing of personal data if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program and provided that such incentive practices are not unjust, unreasonable, coercive, or usurious in nature. The consent may be revoked by the consumer at any time.

(d) Process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in accordance with the Children's Online Privacy Protection Act, 15 U.S.C. ss. 6501 et seq. for a known child under the age of 13.

(3) Paragraph (2)(c) may not be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out under s. 501.705(2) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(4) A controller that operates a search engine shall make available, in an easily accessible location on the web page which does not require a consumer to log in or register to read, an up-to-date, plain language description of the main parameters that are individually or collectively the most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. Algorithms are not required to be disclosed nor is any other information that, with reasonable certainty, would enable deception of or harm to consumers through the manipulation of search results.

501.713 Data protection assessments.—

(1) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(a) The processing of personal data for purposes of targeted advertising.

(b) The sale of personal data.

(c) The processing of personal data for purposes of profiling if the profiling presents a reasonably foreseeable risk of:

1. Unfair or deceptive treatment of or unlawful disparate impact on consumers;

2. Financial, physical, or reputational injury to consumers;

3. A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or

4. Other substantial injury to consumers.

(d) The processing of sensitive data.

(e) Any processing activities involving personal data which present a heightened risk of harm to consumers.

(2) A data protection assessment conducted under subsection (1) must do all of the following:

(a) Identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce such risks.

(b) Factor into the assessment:
1. The use of deidentified data;
2. The reasonable expectations of consumers;
3. The context of the processing; and
4. The relationship between the controller and the consumer whose personal data will be processed.
(3) The disclosure of a data protection assessment in compliance with a request from the Attorney General pursuant to s. 501.72 does not constitute a waiver of attorney-client privilege or work-product protection with respect to the assessment and any information contained in the assessment.
(4) A single data protection assessment may address a comparable set of processing operations which include similar activities.
(5) A data protection assessment conducted by a controller for the purpose of compliance with any other law or regulation may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.
(6) This section applies only to processing activities generated on or after July 1, 2023.

501.72 Enforcement and implementation by the Department of Legal Affairs.—
(1) A violation of this part is an unfair and deceptive trade practice actionable under part II of this chapter solely by the Department of Legal Affairs. If the department has reason to believe that a person is in violation of this section, the department may, as the enforcing authority, bring an action against such person for an unfair or deceptive act or practice. For the purpose of bringing an action pursuant to this section, ss. 501.211 and 501.212 do not apply. In addition to other remedies under part II of this chapter, the department may collect a civil penalty of up to $50,000 per violation. Civil penalties may be tripled for any of the following violations:
(a) A violation involving a Florida consumer who is a known child. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age.
(b) Failure to delete or correct the consumer's personal data pursuant to this section after receiving an authenticated consumer request or directions from a controller to delete or correct such personal data, unless an exception to the requirements to delete or correct such personal data under this section applies.
(c) Continuing to sell or share the consumer's personal data after the consumer chooses to opt out under this part.
(2) After the department has notified a person in writing of an alleged violation, the department may grant a 45-day period to cure the alleged violation and issue a letter of guidance. The 45-day cure period does not apply to an alleged violation of paragraph (1)(a). The department may consider the number and frequency of violations, the substantial likelihood of injury to the public, and the safety of persons or property in determining whether to grant 45 calendar days to cure and the issuance of a letter of guidance. If the alleged violation is cured to the satisfaction of the department and proof of such cure is provided to the department, the department may not bring an action for the alleged violation but, in its discretion, may issue a letter of guidance that indicates that the person will not be offered a 45-day cure period for any future violations. If the person fails to cure the alleged violation within 45 calendar days, the department may bring an action against such person for the alleged violation.

(3) Any action brought by the department may be brought only on behalf of a Florida consumer.
(4) By February 1 of each year, the department shall make a report publicly available on the department's website describing any actions taken by the department to enforce this section. The report must include statistics and relevant information detailing all of the following:
(a) The number of complaints received and the categories or types of violations alleged by the complainant.
(b) The number and type of enforcement actions taken and the outcomes of such actions, including the amount of penalties issued and collected.
(c) The number of complaints resolved without the need for litigation.
(d) For the report due February 1, 2024, the status of the development and implementation of rules to implement this section.
(5) The department shall adopt rules to implement this section, including standards for authenticated consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf.
(6) The department may collaborate and cooperate with other enforcement authorities of the Federal Government or other state governments concerning consumer data privacy issues and consumer data privacy investigations if such enforcement authorities have restrictions governing confidentiality at least as stringent as the restrictions provided in this section.
(7) Liability for a tort, contract claim, or consumer protection claim unrelated to an action brought under this section does not arise solely from the failure of a person to comply with this part.
(8) This part does not establish a private cause of action.
(9) The department may employ or use the legal services of outside counsel and the investigative services of outside personnel to fulfill the obligations of this section.
(10) For purposes of bringing an action pursuant to this section, any person who meets the definition of controller as defined in this part who collects, shares, or sells the personal data of Florida consumers is considered to be engaged in both substantial and not isolated activities within this state and operating, conducting, engaging in, or carrying on a business, and doing business in this state, and is, therefore, subject to the jurisdiction of the courts of this state.

ADDENDUM

Definitions

A. "Company", "companies," or "Shein" as used herein means the addressee/recipients of this subpoena, their parents, branches, departments, divisions, affiliates, subsidiaries, retail outlets, stores, franchises, successors, or predecessors, whether wholly owned or not, including, without limitation, any organization or entity in which said addressees have a management or controlling interest, together with all present and former officers, directors, agents, employees, sales people, brokers, representatives or anyone else acting or purporting to act, on behalf of the above-identified persons or entities, or through which **Shein US Services, LLC** may have conducted business. The term, "affiliate," for purposes of this definition, includes, but is not limited to, Shein Group, Ltd.; Shein Distribution Corporation, a Delaware corporation; Shein Technology LLC, a Delaware limited liability company; Roadget Business Pte Ltd., a Singapore Company; and Zoetop Business Co., Limited, a Hong Kong SAR China Private Limited Company. The term "you" and "your" shall be synonymous with "company," "companies" and "Shein."

B. "Control" as used herein shall have the same meaning as the terms "control" or "controlled" defined in Florida Statute Section 501.702(1).

C. "Document" or "documents" as used herein shall include all paper records and all electronically stored information, including the original and any non-identical copy (whether different from the original because of notations on such copy or otherwise, and including all draft versions of the original), of any written, recorded, or graphic matter, however produced or reproduced, including, but not limited to, all correspondence, communications (as defined below in Paragraph G), web pages, social media communications, photographs, contracts (including drafts, proposals, and any and all exhibits thereto), drafts, minutes and agendas, memoranda (including inter and intra-office memoranda, memoranda for file, pencil jottings, diary entries, desk calendar entries, reported recollections, and any other written form of notation of events or intentions), transcripts and recordings of conversations and telephone calls, audio and video media files, books of account, ledgers, publications, professional journals, invoices, financial statements, purchase orders, receipts, canceled checks and all other paper or electronic documentary material of any nature whatsoever, together with any attachments thereto or enclosures therewith.

D. The term "any" shall be construed as synonymous with "all" and shall be all inclusive.

E. The connectives "and" and "or" shall be construed either disjunctively or conjunctively, whichever makes the request more inclusive.

F. "Child" means an individual younger than 18 years of age.

G. "Communication" or "communications" means any act, action, oral speech, written correspondence, contact, expression of words, thoughts, or ideas, or transmission or exchange of data or other information to another person, whether orally, person to person, in a group, by telephone, letter, personal delivery, intercom, fax, e-mail, text message, social media, or any other process, electric, electronic or otherwise in any medium. All such communications in writing shall include, without limitation, printed, typed, handwritten, or other readable documents.

H. "Person" means any individual and all entities, and, without limiting the generality of the foregoing, includes natural persons, employees, contractors, agents, consultants, vendors, telemarketers, consumers, customers, officers, directors, successors, assigns, joint owners, associations, partnerships, companies, joint ventures, corporations, affiliates, trusts, trustees, escrow agents and estates, and all groups or associations of persons.

I. "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

J. "Personal data" means any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

K. "Sensitive data" means a category of personal data which includes any of the following:
   1) Personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.
   2) Genetic or biometric data processed for the purpose of uniquely identifying an individual.
   3) Personal data collected from a known child.
   4) Precise geolocation data.

L. "Related to" or "relating to" means in whole or in part constituting, containing, concerning, embodying, reflecting, discussing, describing, analyzing, identifying, stating, referring to, setting forth, dealing with, or in any way pertaining to.

Instructions

M. This Subpoena is for the production of all responsive documents and information in your possession, custody or control regardless of whether such documents or information is possessed directly by you or your directors, officers, agents, employees, representatives, subsidiaries, managing agents, affiliates, investigators, or by your attorneys or their agents, employees, representatives, or investigators.

N. Unless otherwise specified, original documents must be produced, and the originals of electronic files must be produced in accordance with paragraph U herein. If your "original" is a photocopy, then the photocopy would be and should be produced as the original. Said copy shall be legible and bound or stapled in the same manner as the original.

O. The documents to be produced pursuant to each request should be segregated and specifically identified to indicate clearly the particular numbered request to which they are responsive.

P. If any responsive document or information cannot be produced in full, you are to produce it to the extent possible, indicating which document, or portion of that document, is being withheld, and the reason that document is being withheld.

Q. If a document once existed and has subsequently been lost, destroyed, or is otherwise missing, please provide sufficient information to identify the document and state the details concerning its loss or destruction.

R. Documents not otherwise responsive to this Subpoena shall be produced if such documents mention, discuss, refer to, or explain the documents that are called for by this Subpoena, or if such documents are attached to documents called for by this Subpoena and constitute routing slips, transmittal memoranda, or letters, comments, evaluations, or similar materials.

S. If you do not possess, control, or have custody of any documents responsive to any numbered request set forth below, state this fact by so specifying in your response to said request.

T. The use of the singular form of a word includes the plural and vice versa. In addition, the use of any tense of any verb includes all other tenses of the verb.

U. ***Electronically Stored Information*** (ESI) is to be produced in the form in which it is ordinarily maintained. For example, native files would include email, spreadsheets and word processing files. Responsive documents that exist in electronic format shall be provided in native format (e.g., Microsoft Word files (.doc) or Outlook (.pst), emails, spreadsheets and word processing documents) with standard metadata intact, as outlined below. Prior to any production of responsive data from a structured database (e.g., Oracle, SAP, SQL, MySQL, QuickBooks, etc.), the producing party shall first provide the database dictionary and a list of all reports that can be generated from the structured database. The list of reports shall be provided in native Excel (.xls) format. The database format will be requested for production after both parties agree on the format. Please include sufficient identification of the applicable software program to permit access to, and use of, each document. All attachments must be linked to their electronic documents. Native files should be provided in directories which are identifiable as responsive to a specific document request. All documents produced in native form should be produced on CDROM, DVDROM, External USB, or other similar drive media of a type that can be read by any standard computer. Unless otherwise agreed to, standard metadata in electronically stored information shall be preserved and produced, such as: Custodian, To, From, CC, BCC, Dates and

Times (Sent, Received and Modified), Attachments, Links and Document types. A more complete list can be provided upon request. Questions regarding electronic production should be directed to the Assistant Attorney General whose name appears on this Subpoena. Arrangements will be made for the communication with the appropriate in-house technical expert.

V. If you claim the attorney-client privilege, work-product privilege, or any other privilege, for any document, provide a detailed privilege log that contains at least the following information for each document that you have withheld:

1) The name of each author, writer, sender or initiator of such document or thing, if any;

2) The name of each recipient, addressee or party for whom such document or thing was intended, if any;

3) The date of such document, if any, or an estimate thereof so indicated if no date appears on the document;

4) The general subject-matter as described on such document; if no such description appears, then such other description sufficient to identify said document; and,

5) The claimed grounds for withholding the document, including, but not limited to, the nature of any claimed privilege and grounds in support thereof.

W. TRADE SECRET PROTECTION. In the event you seek to assert trade secret protection under Florida Statutes section 119.0715, or other applicable Florida Statutes, for each document for which trade secret protection is claimed:

1) Provide prior to, or simultaneous with, production of the document at issue, a sworn affidavit from a person with knowledge as to the basis for the trade secret claim, which complies with the following requirements:

a. The affidavit should specify the bates range of the claimed trade secret documents at issue, generally describe the documents at issue, and provide evidence of the application of the trade secret exemption.

b. The affidavit should attach a certification (similar in form to a traditional privilege log) that identifies the following information for each separate claimed trade secret document: (i) the bates range of the document; (ii) a description of the document sufficient to determine the application of the trade secret exemption; and (iii) the specific element(s) or provision(s) of section 688.002 that render the document at issue a trade secret exempted from public records.

2) Segregate and separately label the documents claimed as trade secrets as follows:

a. Documents produced electronically should be produced on separate CD or electronic media clearly labeled "Trade Secret" on the physical media as well in the title of the electronic folder or file;

b. Documents produced in hard copy should be separated and each clearly labeled "Trade Secret."

3) Any challenge to the application of the trade secret exemption shall be rebutted, if at all, only by you and not by the Office of the Attorney General, whose involvement shall be limited solely to providing notice to you of any challenge to your claim of trade secret protection. To the extent you seek to assert a trade secret exemption in connection with a public records request to the Office of the Attorney General, you shall be obligated to seek an appropriate protective order or otherwise establish the applicability of the trade secret claim and exemption. Failure to do so shall render the documents subject to production under any applicable public records requirements and not protected by a trade secret claim.

X. All document destruction or retention policies and practices and electronic file deletion or disk management policies and practices (including, but not limited to, reformatting practices) that could have the effect of altering or deleting information requested by this Subpoena should be suspended.

1) Because electronically stored information is an important and irreplaceable source of evidence, you must take appropriate steps to preserve all potentially relevant documents within your control or [practical ability to access], which includes, but is not limited to, preserving information from computer systems, removable or portable electronic media (like CDs/DVDs, USB drives), e-mail, text/instant messaging, "tweets" and other electronic correspondence at work and other locations, word processing documents, spreadsheets, databases, calendars, telephone logs, cell phones, voicemail, blogs, social media, internet usage files, website data, personal computers/laptops, personal data assistants (PDAs), servers, and archives/backup files, as well as other tangible documentation that will be relevant to the discovery of admissible evidence in this matter, so as to avoid any potential claims for spoliation of evidence. This request pertains not only to documents that are directly responsive to this Subpoena, but to all other documents that relate to the subject of our investigation as well.

2) Preservation of electronic data in its native format is essential, as a paper printout of text contained in a computer file does not completely reflect all information contained within an electronic file. Additionally, due to its format, electronic evidence can be easily altered, deleted, corrupted or otherwise modified. Accordingly, you are required to take every reasonable step to preserve this information until the resolution of this matter. This includes, but is not limited to, the following obligations:

a) Discontinue all data destruction and overwriting/recycling processes of relevant data;

b) Preserve passwords, decryption procedures (and accompanying software), access codes, ID codes, etc.; and

c) Maintain all pertinent information and tools needed to access, review and reconstruct all requested

or potentially relevant electronic data.

3) Your obligations under the law are ongoing and should be considered in force and effect until the resolution of this matter. Accordingly, with regard to electronic data and documents that are created subsequent to the date of this Subpoena, relevant evidence is not to be destroyed or overwritten and you should take whatever steps are necessary to avoid destruction of potentially-relevant evidence.

WHEREFORE YOU ARE HEREBY COMMANDED TO PRODUCE:

Electronic production is requested*. The time-period applicable to the following requests is **January 1, 2021**, **through the date upon which the response to this Subpoena is due and/or actually provided** to the Office of the Attorney General, whichever occurs later in time. Ensure all documents produced are Bates labeled.

To prevent any potential dissemination of sensitive information, please do not include any personal information in your responses and/or supporting documentation.

When producing documents, index the documents to correspond to each document request.

Information to be Produced:

1. Documents sufficient to show the direct or indirect relationship(s) between:
    a. Shein U.S. Services, LLC and Shein Group Ltd. ("Shein Group");
    b. Shein U.S. Services, LLC and Shein Distribution Corporation ("Shein Distribution");
    c. Shein U.S. Services, LLC and Shein Technology LLC ("Shein Technology");
    d. Shein U.S. Services, LLC and Roadget Business Pte Ltd. ("Roadget"); and
    e. Shein U.S. Services, LLC and Zoetop Business Co. ("Zoetop").
2. All documents related to the collection, processing, sharing, sale or disclosure of personal data by or between any of the entities listed in Request No. 1.
3. Copies of all marketing, advertising, or promotional materials that reference consumer privacy, data collection, data sharing, data retention, data deletion, or cybersecurity practices.
4. Copies of all consumer-facing policies regarding privacy, cookies, data collection, data sharing, data retention, data deletion, and cybersecurity.
5. All documents identifying the location(s) where U.S. personal data, in particular Florida personal data, is being stored.
6. Copies of all documents identifying all third parties with whom personal data has been shared, sold, or disclosed, including but not limited to, contracts requiring data privacy or cybersecurity obligations.

7. Copies of all documents showing what information is being shared with any foreign and/or domestic government entity.

8. Copies of all data cybersecurity policies.

9. Any documents related to the claim on the company's website at https://www.sheingroup.com/privacy-policy/ stating: "When you access or use our Services, **your personal data may be processed or transferred outside the country where you reside, including to the United States, China and/or Singapore.**"

10. Any documents related to the claims on the company's website at https://www.sheingroup.com/our-business/operating-responsibly/#data-security-and-privacy stating:

a. "We use advanced security technologies to protect our global digital systems and — most importantly — our customers' data."

b. "We do not sell or share customer data with anyone."

c. "We are committed to only collecting and using the minimum amount of data necessary to provide our services."

d. "Our systems and controls are aligned to standards set by the International Standards Organization (ISO), National Institute of Standards and Technology (NIST), and the Payment Card Industry's Digital Security Standard (PCI DSS)."

e. "We also partner with third-party experts and top security firms to conduct regular risk assessments based on these internationally recognized security standards and frameworks."

11. Any document prepared by Shein that complies with Section 501.713, Florida Statutes, regarding a data protection assessment.

12. Documents sufficient to show Shein's 2025 total global gross annual revenue.

13. Documents sufficient to show the three largest sources of Shein's 2025 total global gross annual revenue, including the amount of revenue from each source.

14. Documents sufficient to show the relationship between Shein and any consumer smart speakers sold or offered for sale in the United States.

15. Documents sufficient to show the relationship between Shein and all app stores and other digital distribution platforms, including, but not limited to the Apple App Store and Google Play Store, that are accessed by customers in the United States.

16. Documents sufficient to show whether Shein operates an app store or a digital distribution platform, and if Shein operates such a store or platform, documents sufficient to identify the different software applications available for consumers to download and install. In responding to this request with respect to identifying the software applications, Shein may provide a list, spreadsheet, or other summarizing document in lieu of the actual documents requested.

17. Documents sufficient to identify the name of any persons or entities which may exercise control over Shein.

18. Documents sufficient to show how a consumer may exercise their rights enumerated in Section 501.705, Florida Statutes.

19. All consumer requests or complaints to You regarding their rights enumerated in Section 501.705, Florida Statutes.

20. Copies of all documents relating to how a consumer may choose to consent to the processing of their sensitive data prior to You processing their personal data.

21. Copies of all documents showing how a Child consumer may choose to consent to the processing of their sensitive data prior to You processing their personal data.

22. Copies of all documents showing how a consumer may consent to the sale of their sensitive data prior to You selling the sensitive data.

23. Copies of all documents relating to how a Child consumer may consent to the sale of their sensitive data prior to You selling the sensitive data.

24. Documents related to any product reported by Shein to the Consumer Product Safety Commission (CPSC) pursuant to the mandatory reporting requirements of Section 15 of the Consumer Product Safety Act (CPSA), including, but not limited to, documents relating to the CPSC's evaluation of the reported information, actions taken by Shein or the CPSC regarding the product, and the outcome.

25. Documents and communications related to all Notices of Violation received by or copied to Shein from the CPSC, regardless of whether the referenced product was sold by Shein or by a third-party seller on Shein's platform, including, but not limited to, documents showing Shein's actions taken in response to such Notices and the outcomes.

26. Documents sufficient to show Shein's plan or process for conducting product recalls, including, but not limited to, exemplars of stop-sale notices, Shein's process for blocking online sales, any audit process of Shein's recall plan, any reverse logistics process to ensure recalled products do not return to the market, and training materials.

27. Shein's Restricted Substances List, Manufacturing Restricted Substances List, and Approved Fabrics List, however designated, including documents sufficient to show the current and prior versions of the lists, the dates any substances or fabrics were added or removed from the lists, the reason or methodology for adding or removing a substance or fabric from the lists, and documents sufficient to show who has or had authority to add or remove substances or fabrics from the lists.

28. With respect to the following product safety standards, policies, and lists imposed by Shein (separately and together, "Product Safety and Responsible Sourcing Standards"), documents relating to Shein's **monitoring** and **enforcement** of compliance by, and related compliance **trainings** to, suppliers, subcontractors, and sellers, and documents relating to Shein's **verifying of the truthfulness and authenticity** of any certifications of compliance or supply chain chain-of-custody documents provided by its suppliers, subcontractors, and sellers, where all such documents should include, but not be limited to, any policies, procedures, guidance, manuals, checklists, agreements, training materials, and those related to the "dynamic evaluation of vendors" process claimed to occur by Shein on Shein's website at https://www.sheingroup.com/corporate-news/company-updates/shein-further-intensifies-product-safety-quality-protocols-targets-2-5-million-tests-in-2025/:

a. Restricted Substances List;

b. Manufacturing Restricted Substances List;

c. Approved Fabrics List;

d. Supplier Responsibility Standards;

e. Supplier Code of Conduct;

f. Responsible Sourcing Policy ("SRS");

g. Seller Code of Conduct;

h. Restricted Products Policy; and

i. Any other product safety-related standards imposed by Shein.

29. Documents sufficient to show all entities against whom Shein has taken any level of enforcement or remedial action for violating the above Product Safety and Responsible Sourcing Standards, and all documents and communications relating to such action.

30. Documents relating to Shein's claim on the company's website, https://www.sheingroup.com/corporate-news/company-updates/shein-further-intensifies-product-safety-quality-protocols-targets-2-5-million-tests-in-2025/, that "[a]dditionally, as of April 2025, all fabrics that could be used in SHEIN brand children's apparel must be tested against chemical standards and flammability upon onboarding[,]" which documents should include, but not be limited to, policies, procedures, and any documents sufficient to identify these fabrics, the test results relating to these fabrics, and the rejection of any such fabrics from use in children's apparel, along with documents sufficient to show how Shein ensures unapproved fabrics have not been used in children's apparel sold by Shein or third-party sellers on its platform and how Shein processes the removal of such items from sale on its platform.

31. Documents sufficient to show the types of information that must be submitted by suppliers, subcontractors, and sellers to Shein in compliance with Shein's requirement that these entities "submit documentation for products from categories such as . . . children's toys, children's products, baby products, . . . and textiles with specific regulatory requirements for SHEIN's system checks and manual reviews[,]" as stated by Shein on its website at https://www.sheingroup.com/corporate-news/company-updates/shein-further-intensifies-product-safety-quality-protocols-targets-2-5-million-tests-in-2025/, along with documents sufficient to describe Shein's system checks and manual review process.

32. Exemplar of the checklist, however designated, used by Shein, or any third-parties hired by Shein, to conduct SRS audits of suppliers and subcontractors as referenced on Shein's website at https://www.sheingroup.com/our-business/our-supply-chain/#our-supply-chain-standards.

33. Documents sufficient to show the suppliers and subcontractors for whom Shein, or any third-parties hired by Shein, conducted SRS audits and the outcome of such audits, along with documents relating to any enforcement action taken with respect to the outcome of such audits, and copies of the completed SRS audit checklist for any suppliers or subcontractors who failed to meet any standards evaluated during the audit.

34. All documents to support the claims on the company's website at https://www.sheingroup.com/corporate-news/company-updates/shein-further-intensifies-product-safety-quality-protocols-targets-2-5-million-tests-in-2025/ stating:

a. "SHEIN's dedicated compliance team closely monitors compliance regulations around the world to update and maintain the company's standards and policies on a regular basis."

b. "Product safety tests, including chemical tests, are carried out throughout the sales cycle, in collaboration with leading third-party testing agencies."

35. With respect to children's toys, children's apparel, and baby products tested by Shein using third-party testing agencies, documents sufficient to identify all products that failed to meet Shein's and regulating agencies' rules and standards, which identification information should include the product name, SKU, manufacturer name, and seller name, the reason for the failure, date of the test, and any actions taken by Shein relating to such products.

36. Documents sufficient to show the names and addresses of third-party sellers for whom Shein has terminated the ability to sell products on Shein's platform and the reason for such termination.

37. Documents sufficient to identify consumers, which identification should include a consumer's name, telephone number, email address, and physical address, who were sold products:

a. indicated in response to Request 24 above;

b. that were the subject of the Notices of Violations indicated in response to Request 25 above;

c. for which Shein initiated a recall;

d. from entities indicated in response to Request 29 above;

e. that had any materials deriving from suppliers or subcontractors indicated in response to Request 33 above as having failed to meet any standards evaluated in an SRS audit; and

f. from third-party sellers indicated in response to Request 36 above where the reason for termination relates to violations of Shein's Product Safety and Responsible Sourcing Standards and United States product safety laws and forced labor laws, including, but not limited to the CPSA, the Consumer Product Safety Improvement Act, and the Uyghur Forced Labor Prevention Act.

In responding to this request, Shein may provide a list, spreadsheet, or other summarizing document in lieu of the actual documents requested, provided such summarizing document shall, for each listed consumer, indicate the subparagraph above pursuant to which Shein is identifying the consumer.

38. For each consumer indicated in response to Request 37 above, documents sufficient to show the product(s) sold to the consumer and the amount paid by each consumer for the product(s).

39. Documents sufficient to show Shein's gross sales and gross revenue derived from its own and third-party sellers' selling of products to consumers in the State of Florida.

40. Exemplars of all current and previously used Master Seller Agreements Shein requires third-party sellers to sign.

41. Documents sufficient to show the number of third-party sellers currently selling products in the United States of America using Shein's platform.

42. Reports, memorandums, or presentations from Shein's Centre of Innovation for Garment Manufacturing regarding any research or development of systems, programs, applications, policies or procedures relating to Product Safety Standards and the monitoring and enforcement of such Product Safety and Responsible Sourcing Standards.

43. Exemplars of each type of document suppliers are required to submit to Shein's Traceability Management System (TMS), and screenshots showing the TMS user interfaces and the types of information documented in the TMS.

44. Documents sufficient to show how Shein ensures that deadstock materials obtained through its relationship with Aloquia (formerly Queen of Raw) does not contain cotton derived from the Xinjiang Uyghur Autonomous Region.

45. Documents sufficient to show the names and addresses of all suppliers who operate in or use cotton from the Xinjiang Uyghur Autonomous Region.

46. To the extent not produced in response to the requests above, documents related to Shein's compliance with United States product safety laws and forced labor laws, including, but not limited to the CPSA, the Consumer Product Safety Improvement Act, and the Uyghur Forced Labor Prevention Act.

47. Documents sufficient to identify all current and former employees, independent contractors, or agents of Shein involved in verifying and enforcing compliance with Shein's Product Safety and Responsible Sourcing Standards and United States consumer product safety and forced labor laws, which identification information shall include the name, job title, dates of employment, and known contact information for those who are identified. In responding to this request, Shein may provide a list, spreadsheet, or other summarizing document in lieu of the actual documents requested.

48. Documents related to complaints from consumers or inquiries from government agencies related to product safety or supply chain sourcing of cotton from the Xinjiang Uyghur Autonomous Region or from other use of forced labor, and the actions taken and ultimate resolution with respect to such complaints and inquiries.

49. Documents related to any grievances submitted to Shein by any Shein employee, independent contractor, or agent related to product safety or the sourcing of cotton from the Xinjiang Uyghur Autonomous Region.

Responsive documents that exist in electronic format shall be provided in native format (e.g., Microsoft Word files (.doc) or Outlook e-mails(.pst), and Microsoft Excel spreadsheets (.xls).

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

CERTIFICATION AFFIDAVIT OF RECORDS OF
REGULARLY CONDUCTED BUSINESS ACTIVITY

I, _____, the undersigned declarant, have personal knowledge of the facts set forth below and hereby declare, certify and state the following:

1) I am employed by _____ referred to herein as "the Business" (the term Business can include a business, agency, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit).

2) My title is _____.

3) I am familiar with the records of the Business. I have authority to certify the authenticity of the records produced by the Business and attached hereto.

4) The documents attached hereto are originals or true copies of records that:

   a) Were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

   b) Were kept in the course of the regularly conducted activity of the Business; and,

   c) Were made as a regular practice in the course of regularly conducted activity of the Business.

I certify under penalty of perjury that the foregoing is true and correct.

FURTHER AFFIANT SAYETH NAUGHT.

_____
Signature

STATE OF _____

COUNTY OF _____

The foregoing instrument was acknowledged before me by means of [____] physical presence or [_____] online notarization this _____ day of _____(month), 202___, by _____ (name of person making this certification affidavit) as _____ (title or type of authority) for _____ _____ _____ (name of business/agency/association party on behalf of whom instrument was executed).

(NOTARY SEAL)

_____
NOTARY PUBLIC, (signature)

Personally Known _____ OR Produced Identification _____

Type of Identification Produced _____