BEFORE THE OFFICE OF THE
UNITED STATES TRADE REPRESENTATIVE

PETITION FOR RELIEF UNDER SECTION 301 OF THE TRADE ACT OF 1974, AS AMENDED

REPUBLIC OF KOREA'S ACTS, POLICIES, AND PRACTICES TARGETING COUPANG, INC.

ON BEHALF OF

Greenoaks Capital Partners LLC and Altimeter Capital Management, LP

COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, N.W.
Washington, DC 20001-4956
Tel: +1 (202) 662 6000

Counsel to Greenoaks Capital Partners LLC and Altimeter Capital Management, LP

January 22, 2026

TABLE OF CONTENTS

Page

I. INTRODUCTION

Greenoaks Capital Partners LLC ("Greenoaks") and Altimeter Capital Management, LP ("Altimeter") (collectively, "Petitioners") respectfully submit this petition under Section 302(a) of the Trade Act of 1974, as amended, to request that the Office of the United States Trade Representative ("USTR") investigate and respond to the unreasonable and discriminatory acts, policies, and practices of the Government of the Republic of Korea, particularly those targeting U.S. technology and online retail company Coupang Inc. and its wholly-owned Korean subsidiary Coupang Corp. (collectively, "Coupang"). Greenoaks and Altimeter hold equity interests in Coupang valued at more than $1.5 billion.

The Korean Government is currently in the midst of a whole-of-government assault on Coupang. Operating the largest online retail marketplace in South Korea, Coupang has emerged as a U.S. champion and leading innovator in e-commerce. Coupang is often referred to as the "Amazon of South Korea." The company is widely recognized for its "Dawn Delivery" service, which guarantees next-morning delivery for orders placed by midnight. This service is supported by Coupang's proprietary logistics network, comprising more than 100 fulfillment and logistics centers, advanced automation and software systems, and a fleet of over 25,000 delivery vehicles operating nationwide.

Coupang's commercial success and leading role in the transformation of the Korean e-commerce sector were made possible by not only cutting-edge U.S. technologies, but also by U.S. investors such as Greenoaks and Altimeter. The Korean Government's unreasonable and discriminatory actions targeting Coupang therefore directly impair substantial U.S. economic interests and threaten U.S. innovation and investment in the technology sector in Korea.

While Coupang should be a symbol of U.S.-Korea partnership, instead it reflects Korea's disrespect for fair and transparent regulatory practices, particularly when it comes to U.S. technology companies. The Korean Government has used a limited data breach in November 2025 as a pretext for launching a whole-of-government pressure campaign, unjustifiably and arbitrarily singling out Coupang for discriminatory treatment and disproportionate punishment.

In November 2025, Coupang discovered a data incident that was perpetrated by a former Coupang employee—a Chinese national based in China.[1] The breach was limited in scope, with approximately 3,000 user accounts downloaded by the threat actor. By all objective accounts the breach was promptly contained, in part through Coupang's cooperation with Korean authorities. Korean officials, however, have seized upon the incident to engage in a hostile campaign towards the company.

Over a matter of weeks, the Korean Government's hostility has escalated into a coordinated effort to cripple Coupang's operations. The Korean Government has disseminated false information with respect to the scale and sensitivity of the data involved in the breach, threatened Coupang with unjustifiable record penalties, weaponized investigative and enforcement authorities that bear no relation to the alleged conduct, referred senior executives (including U.S. nationals) for criminal prosecution, called for travel bans that would prevent U.S. executives from leaving Korea, and threatened the revocation of Coupang's business license. The Government's actions

[1] Coupang, Form 8-K/A, Item 1.05 (Dec. 29, 2025), https://ir.aboutcoupang.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=19025871 **(Ex. 01)**; *see also* Lee Mi-ji, *Coupang Recovers Leaker's Devices, Confirms No External Data Transmission*, The Chosun Daily (Dec. 25, 2025), https://www.chosun.com/english/industry-en/2025/12/25/KQK4652CFVGH7MX5WRGMOJQURQ/ [https://perma.cc/R5A8-BVBU] **(Ex. 81)**.

are not only impairing Coupang's operations, but also eroding Coupang's customer base, with some consumers shifting to Korean competitors.[2]

The Korean Government's relentless and disproportionate reaction flows from Korea's highest office. Led by President Lee Jae Myung's bold pronouncement that Coupang should face penalties so severe that it fears collapse,[3] the governmental response to a limited data breach has involved investigations by more than a dozen federal agencies, multiple inter-ministerial task forces, and the mobilization of hundreds of investigators and auditors. This overwhelming response bears no rational relationship to the objective facts of the data incident, and it is wildly out of proportion with governmental responses to similar incidents involving Korean and Chinese companies.

The bottom line is that the Korean Government is singling out a successful U.S. innovator, misusing the criminal process and regulatory authorities as instruments of economic coercion rather than legitimate enforcement, and engaging in unfair and discriminatory treatment that bears no justifiable connection to the alleged government concern of addressing a limited data breach.

Particularly in light of Korea's recent commitments to the U.S. Government not to discriminate against U.S. technology companies,[4] Korea's disproportionate attacks on Coupang

---

[2] Korea Bizwire, *Coupang Data Breach Triggers Shift in Korea's E-Commerce Landscape*, The Korea Bizwire (Jan. 21, 2026), http://koreabizwire.com/coupang-data-breach-triggers-shift-in-koreas-e-commerce-landscape/342492 [https://perma.cc/4APR-8NGH] **(Ex. 02)**.

[3] Kim Tae-jun, *Exclusive: Presidential Office Prohibits Staff From Contacting Coupang*, The Chosun Daily (last updated Dec. 25, 2025), https://www.chosun.com/english/national-en/2025/12/25/RRXZA7V2EJBGZJHRZBZO7N7BL4/; The Dong-A Ilbo, *Lee calls for tougher fines after Coupang data leak* (Dec. 13, 2025), https://www.donga.com/en/article/all/20251213/6009706/1 [https://perma.cc/NY3C-5BKF] **(Ex. 03)**.

[4] U.S. Trade Representative, *Fact Sheet: The United States and Korea Agree to the Korea Strategic Trade and Investment Deal* (Nov. 2025), https://ustr.gov/about/policy-offices/press-office/fact-sheets/2025/november/fact-
(continued…)

cannot be ignored. The explicit targeting of U.S. executives for criminal referral and travel restrictions represents an especially serious escalation, raising concerns not only about discrimination against U.S. commerce, but also about the personal safety and legal exposure of U.S. nationals doing business in Korea.

Although this petition focuses on the Korean Government's unreasonable and discriminatory actions against Coupang specifically, this attack is part of a broader and persistent pattern of conduct by the Korean Government. The U.S. Government, U.S. companies, other interested stakeholders, and the press have documented the Korean Government's weaponization of investigations and enforcement actions against U.S. technology companies. These discriminatory and unjustified attacks have been exacerbated by recent legislative developments in Korea that specifically target U.S. technology companies. Coupang's case thus presents a paradigmatic example of a systemic policy and practice that burdens or restricts U.S. commerce within the meaning of Section 301 of the Trade Act of 1974 ("Section 301"), by rendering U.S. technology companies operating in Korea less competitive, less innovative, and less secure. Korea's whole-of-government campaign against Coupang is not only impairing substantial U.S. economic interests, but also establishing a dangerous precedent that commercial success by U.S. companies in Korea may lead to political retaliation, regulatory harassment, and personal legal jeopardy for U.S. executives.

* * *

As set forth in this petition, Korea's acts, policies, and practices are actionable under Section 301. Part II of this petition outlines the legal standard for action under Section 301 and

---

sheet-united-states-and-korea-agree-korea-strategic-trade-and-investment-deal [https://perma.cc/9N3H-8WNL] **(Ex. 04)**.

Petitioners' standing to submit a Section 301 petition. Part III details Korea's acts, policies, and practices, which are unreasonable, discriminatory, and burden or restrict U.S. commerce, not only with regard to the U.S. technology industry in general, but also with regard to Coupang in particular. Part IV requests specific countermeasures to address the Korean Government's pattern of discriminatory and unreasonable conduct against Coupang. Part V addresses Petitioners' request for a public hearing and identifies other forms of relief sought by the Petitioners under the Trade Act of 1974 or any other provision of law.

II. LEGAL STANDARD

Under Section 301(b), the U.S. Trade Representative may take "all appropriate and feasible action" where he determines that "an act, policy, or practice of a foreign country is unreasonable or discriminatory and burdens or restricts United States commerce," and that an "action by the United States is appropriate."[5] Section 301(d)(5) defines "discriminatory" to "include . . . any act, policy, and practice which denies national or most-favored nation treatment to United States goods, services, or investment."[6] Under Section 301(d)(3)(A), "unreasonable" refers to an act, policy, or practice that, "while not necessarily in violation of, or inconsistent with, the international legal rights of the United States, is otherwise unfair and inequitable."[7] The statute further provides that, in determining if a foreign country's practices are unreasonable, "reciprocal opportunities" offered to foreign firms in the United States "shall be taken into account, to the extent appropriate."[8]

---

[5] 19 U.S.C. § 2411(b).

[6] 19 U.S.C. § 2411(d)(5).

[7] 19 U.S.C. § 2411(d)(3)(A).

[8] 19 U.S.C. § 2411(d)(3)(D).

Under Section 302(a), any "interested person" can file a petition with USTR requesting that an action be taken under Section 301, with the petition "setting forth the allegations in support of the request."[9] "Interested persons" is defined broadly for the purpose of filing a petition, as it "includes, but is not limited to, domestic firms and workers, representatives of consumer interests, United States product exporters, and any industrial user of any goods or services that may be affected" by unfair foreign trade practices.[10] Petitioners Greenoaks and Altimeter are, respectively, a limited liability company and a limited partnership, constituted under the laws of Delaware. Greenoaks and Altimeter are interested persons under the statute because their economic interests are adversely affected by the Korean Government's acts, policies, and practices targeting Coupang. In particular, Greenoaks and Altimeter manage significant investments on behalf of investors in Coupang, Inc., the U.S. parent company of Coupang Corp., its wholly owned Korean subsidiary. In addition to being Korea's largest online retail company, Coupang sources billions of dollars in products from U.S. companies for sale on its retail sites in Korea and throughout the Indo-Pacific.[11] In submitting this petition, Greenoaks and Altimeter seek to protect U.S. economic interests associated with the investments they manage in Coupang against the escalating existential threat posed by recent actions of the Korean Government against Coupang.

Petitioners note that they are providing herein information reasonably available to them, and they are providing the information they have at this time, including information on the laws, regulations, and other measures that are the subject of this petition. Given the urgency of the

---

[9] 19 U.S.C. § 2412(a).

[10] 19 U.S.C. § 2411(d)(9).

[11] Coupang, *Meet Coupang: The U.S. Tech Company Driving American Exports*, https://www.aboutcoupang.com/English/news/news-details/2025/meet-coupang-the-u-s-tech-company-driving-american-exports/# [https://perma.cc/YZN3-8LVH] **(Ex. 05)**.

matter and its ongoing nature, Petitioners reserve the right to supplement this record as additional information becomes available.

III. KOREA'S ACTIONS ARE UNREASONABLE AND DISCRIMINATORY, AND BURDEN OR RESTRICT U.S. COMMERCE UNDER SECTION 301(b)

Korea has a well-established history of targeting U.S. companies in the technology sector for discriminatory and arbitrary treatment and overly aggressive enforcement actions. Emblematic of the Korean Government's disparate treatment of U.S. companies are Korea's actions against Coupang. For years, the Korean Government has selectively weaponized audits, raids, and inspections as tools to undermine Coupang's business. Korea's recent escalation of this hostile campaign and its increased regulatory scrutiny of Coupang only underscores the unfair and unjust nature of Korea's actions, which lack any discernible factual basis or regulatory justification, and are wholly disproportionate to Government actions taken with respect to non-U.S. companies in similar circumstances.

Because this disparate treatment is effectively based on nationality and places U.S. technology companies like Coupang and their investors at a disadvantage relative to domestic competitors and other investors in the Korean market, Korea's actions constitute discrimination under Section 301. Moreover, Korea's acts, policies, and practices are unreasonable because they are directed and supported by the government, and harm not only U.S. technology companies and U.S. investors, but also U.S. innovation and technological leadership, all while Korean companies freely enjoy commercial opportunities and market access in the United States.

A. Korea's History of Discriminatory Treatment of U.S. Businesses

There is no shortage of examples of the Korean Government targeting U.S. companies with overly aggressive enforcement actions. The Korea Fair Trade Commission ("KFTC") routinely

subjects U.S. companies to aggressive tactics.[12] U.S. technology companies, including Coupang, are subject to frequent raids, overly aggressive enforcement, and threats of criminal prosecution that are entirely disproportionate, punish common industry practice, and lead to unfair and unjustified harassment and monetary penalties.[13] Over the last decade alone, a string of U.S. technology companies have found themselves in the KFTC's crosshairs, and U.S. companies have faced some of the largest fines in Korea's history.[14]

---

[12] American Chamber of Commerce Korea, *Policy Talks with KFTC Chairperson* (Dec. 15, 2025), https://www.amchamkorea.org/pp/latest_news/amcham_news/read/?idx=2616 [https://perma.cc/C3NY-EQ4G] (describing a meeting in which the KFTC Chairman addressed concerns about discriminatory investigations and enforcement against U.S. companies) **(Ex. 06)**; U.S. Chamber of Commerce, *Submission to Amb. Greer on Harm from Non-Reciprocal Trade Arrangements*, Annex A, p. 32 (Mar. 11, 2025), https://www.uschamber.com/assets/documents/250311_USChamber_Comments_ForeignTradeBarriers_USTR_FINAL.pdf [https://perma.cc/54B6-E7MH] (noting that "the Korea Fair Trade Commission's arbitrary investigations, rulings, and actions . . . often disproportionately target U.S. companies") **(Ex. 07)**.

[13] *See, e.g.,* Consumer Technology Association, *Comments on the 2026 National Trade Estimate Report*, p. 34 (Oct. 30, 2025), https://www.cta.tech/media/lsyafiqe/cta-comments-to-ustr-on-nte-2026-topics.pdf **(Ex. 08)**.

[14] *See* Nigel Cory & Robert Holleyman, *Safeguarding U.S. Companies from Unfair South Korean Competition Policies*, National Bureau of Asian Research (June 12, 2025), https://www.nbr.org/publication/safeguarding-u-s-companies-from-unfair-south-korean-competition-policies/ **(Ex. 09)**; *see also* Se Young Lee & Stephen Nellis, *South Korea Fines Qualcomm $854 million for Violating Competition Laws*, Reuters (Dec. 28, 2016), https://www.reuters.com/article/world/south-korea-fines-qualcomm-854-million-for-violating-competition-laws-idUSKBN14H05X/ **(Ex. 10)**; Kim Bo-eun, *Korea Fines Google W207 Bil. for Abuse of Market Dominance*, The Korea Times (Sept. 14, 2021), https://www.koreatimes.co.kr/business/tech-science/20210914/korea-fines-google-w207-bil-for-abuse-of-market-dominance [https://perma.cc/B2BV-XMUJ] ("This is the third-largest fine to be imposed by the KFTC on a company for abuse of their dominant market status. Other cases involved Qualcomm, a U.S. semiconductor and telecommunications equipment company.") **(Ex. 11)**; Eun-Young Jeong, *Qualcomm Faces $853 Million Fine from South Korea over Alleged Antitrust Violations*, Wall Street Journal (Dec. 28, 2015), https://www.wsj.com/articles/qualcomm-fined-more-than-850-million-in-south-korea-for-alleged-antitrust-violations-company-to-fight-decision-1482894283 [https://perma.cc/8WJ7-58DY] **(Ex. 12)**; Julie Masson, *Apple Faces Criminal Charges for Obstructing Probe in Korea*, Global Competition Review (Mar. 31, 2021), https://globalcompetitionreview.com/article/apple-faces-criminal-charges-obstructing-probe-in-korea [https://perma.cc/N2EL-AKE4] **(Ex. 13)**; Hyunsu Yim & Heekyong Yang, *South Korea Fines Google $32 Million for Blocking Games on Competing Platform*, Reuters (Apr. 11, 2023), https://www.reuters.com/technology/south-korea-fines-google-32-mln-blocking-release-games-competitors-platform-2023-04-11/ **(Ex. 14)**; Kim Seung-hyeon & Ahn Sang-hyun, *Google's YouTube Music Deal Avoids Sanctions, Shakes S. Korean Streaming Market*, The Chosun Daily (May 23, 2025), https://www.chosun.com/english/industry-en/2025/05/23/C5LAZXN5LJD7LE4FZH4T62ITOI/ [https://perma.cc/TA5G-P6RY] **(Ex. 15)**.

USTR's own statements about Korea's discriminatory e-commerce and digital trade barriers confirm the Korean Government's practice of targeting U.S. companies. For instance, in the 2025 NTE Report, USTR identified a number of barriers to trade in the digital and e-commerce sectors, including Korea's competition policy, restrictions on location-based data, and data localization requirements, among others.[15] USTR's previous NTE Reports similarly identified how Korea's digital policies discriminate against U.S. technology companies.[16] This longstanding practice of the Korean Government explains why, as the U.S. State Department noted in its most recent statement on the investment climate in Korea, "U.S. firms have raised concerns that KFTC

---

[15] *See* U.S. Trade Representative, 2025 National Trade Estimate Report on Foreign Trade Barriers of the President of the United States on the Trade Agreements Program, pp. 252-253 (Mar. 2025), https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf [https://perma.cc/PD4H-RYGT] **(Ex. 16)**; *see also* Senate Committee on Finance, *Response to Senator Questions: The President's 2025 Trade Policy Agenda*, pp. 11-12 (Apr. 8, 2025), https://www.finance.senate.gov/imo/media/doc/responses_to_questions_for_the_record_to_jamieson_greer2.pdf [https://perma.cc/B2WA-NN7Q] (in responding to a question from Senator Young (R-IN) regarding "digital trade barriers abroad" from countries like Korea "that, while framed as neutral, disproportionately target U.S. companies operating at scale," Ambassador Greer confirmed that the United States "will oppose discriminatory measures that target U.S. technology companies," and that he is "exploring using any and all of the tools available to me as the U.S. Trade Representative") **(Ex. 17)**.

Petitioners understand that these data restrictions were promulgated under the Personal Information Protection Act. *See* Personal Information Protection Act (Act No. 19234, Mar. 14, 2023) **(Ex. 18)**; Enforcement Decree of the Personal Information Protection Act (Presidential Decree No. 35343, Feb. 25, 2025) **(Ex. 19)**. Petitioners have attached the English versions of the relevant statutes in this Petition, and are happy to provide Korean language versions upon request.

[16] *See, e.g.*, U.S. Trade Representative, 2024 National Trade Estimate Report on Foreign Trade Barriers of the President of the United States on the Trade Agreements Program, pp. 243 (Mar. 2024), https://ustr.gov/sites/default/files/2024%20NTE%20Report.pdf [https://perma.cc/F8WS-3CM4] **(Ex. 20)**; U.S. Trade Representative, 2023 National Trade Estimate Report on Foreign Trade Barriers of the President of the United States on the Trade Agreements Program, pp. 262-263 (Mar. 2023), https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf [https://perma.cc/YFJ5-Q79Y] **(Ex. 21)**; U.S. Trade Representative, 2019 National Trade Estimate Report on Foreign Trade Barriers of the President of the United States on the Trade Agreements Program, pp. 324-326 (Mar. 2019), https://ustr.gov/sites/default/files/2019_National_Trade_Estimate_Report.pdf [https://perma.cc/S72D-2T46] **(Ex. 22)**.

targets foreign companies with aggressive enforcement."[17] Those concerns are heightened where enforcement is paired with public intimidation campaigns and the prospect of personal legal jeopardy for executives of U.S.-linked firms.

Members of Congress have also expressed consistent concern with Korea's digital policies and regulatory enforcement. A letter from 43 members of Congress in July 2025 identified legislative developments in Korea that "would impose disparate legal and enforcement standards designed to undermine innovative business models and disadvantage successful American companies," while also highlighting that the KFTC's discriminatory investigations "greatly constrain[] U.S. business operations in the Korean market."[18] In May 2025, Representative Carol Miller (R-WV) introduced H.R. 3193, the "United States-Republic of Korea Digital Trade Enforcement Act," which included as the sense of Congress that "South Korea's discriminatory economic policies" are contributing to the U.S. bilateral trade deficit with Korea, and noted that "South Korea is considering additional discriminatory digital regulations that would unduly burden United States businesses while benefitting Chinese technology companies."[19]

Although USTR successfully negotiated a commitment from Korea this past November "to ensure that U.S. companies are not discriminated against and do not face unnecessary barriers in

---

[17] U.S. Dep't of State, *Investment Climate Statements: South Korea*, p. 15 (Sep. 2025), https://www.state.gov/wp-content/uploads/2025/08/638719_2025-Republic-of-Korea-Investment-Climate-Statement.pdf [https://perma.cc/Q22X-Q8F5] **(Ex. 23)**.

[18] *See* Letter from 43 Members of Congress to Ambassador Greer, Secretary Bessent, and Secretary Lutnick (July 1, 2025), https://adriansmith.house.gov/sites/evo-subsites/adriansmith.house.gov/files/evo-media-document/7.1.2025-final-korea-digital-trade-letter.pdf [https://perma.cc/Q9YR-4RAZ] **(Ex. 24)**.

[19] United States-Republic of Korea Digital Trade Enforcement Act, H.R.3193, 119th Cong (2025) **(Ex. 25)**.

terms of laws and policies concerning digital services,"[20] the Korean Government's treatment of Coupang discredits that commitment. The disproportionate attacks on Coupang are irreconcilable with any credible assurance of a stable, rules-based operating environment for U.S. digital commerce and investment.

B. Korea's Unreasonable and Discriminatory Treatment of Coupang

Even against the backdrop of the Korean Government's historic discrimination against U.S. companies, Korea's treatment of Coupang is particularly egregious and uniquely harmful. For years, the Korean Government has selectively weaponized audits, raids, and inspections as tools to undermine Coupang's business. Coupang has faced extraordinary scrutiny from regulators who demand access to its offices, personnel, and records in a way that impairs its ability to run its day-to-day operations. Petitioners are unaware of any similarly situated Korean competitor who has faced regulatory scrutiny anywhere near the same scale or intensity. That discrimination has escalated into a coordinated, whole-of-government campaign in which multiple agencies operate in parallel to overwhelm Coupang's operations and management capacity.

The Korean Government's relentless focus on Coupang for unfair and discriminatory actions is not entirely new. A myriad of government actors, including the Ministry of Employment and Labor ("MOEL"), the KFTC, the Financial Supervisory Service ("FSS"), and the National Tax Service ("NTS") have harassed Coupang in recent years. By way of example, in 2024, the KFTC investigated Coupang under the Monopoly Regulation and Fair Trade Act ("MRFTA") for

[20] White House, *Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae Myung* (Nov. 13, 2025), https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/ [https://perma.cc/KDS5-G7DY] **(Ex. 26)**.

allegedly using its search algorithms and other measures to boost its own products.[21] Coupang was sanctioned with a fine of approximately $100 million, the largest fine ever imposed by Korea on a retailer, and a criminal complaint was filed against the company.[22] By contrast, when Naver, Coupang's Korean-owned competitor, was investigated under the MRFTA regarding similar allegations, its fine was only $23 million (which was later reversed) and there was no criminal referral.[23] This disparate treatment is emblematic of a broader pattern: Korea applies one standard to a successful U.S.-linked innovator and another to powerful domestic competitors.

1. The November 2025 Data Breach

On November 18, 2025, Coupang discovered a data breach and promptly launched an internal investigation. Coupang also disclosed the data breach to the Government and began working closely with Government agencies, especially the National Intelligence Service (the "NIS"), to ensure the breach was contained. Coupang retained leading cybersecurity firms and determined that a former employee had relied on insider knowledge and a restricted "Fallback Key" to forge authentication tokens and access customer data.[24] The investigation confirmed that the former employee had access to millions of accounts, but downloaded and retained user data

---

[21] Petitioners understand that this investigation was conducted pursuant to Korea's Monopoly Regulation and Fair Trade Act (Act No. 20711, Jan. 21, 2025) **(Ex. 27)**; *see also* Enforcement Decree of the Monopoly Regulation and Fair Trade Act (Presidential Decree No. 35382, Mar. 12, 2025) **(Ex. 28)**.

[22] Kwon Soon-wan et al., *Coupang Fined 140 Billion Won For Manipulating Search Results For Private Brands*, The Chosun Daily (Jun. 14, 2024), https://www.chosun.com/english/industry-en/2024/06/14/D6O4KS2P2VF2FGHV2LYVFWW3OI/ [https://perma.cc/9JZ5-XXYR] **(Ex. 29)**.

[23] Nam Hyun-woo, *Naver Fined W26.7 Bil. For Manipulating Search Algorithm*, The Korea Times (last updated Oct. 7, 2020), https://www.koreatimes.co.kr/business/tech-science/20201006/naver-fined-w267-bil-for-manipulating-search-algorithm [https://perma.cc/9UJK-DLYQ] **(Ex. 30)**.

[24] *See* Coupang, Form 8-K/A, Exhibit 99.1 (Dec. 29, 2025), https://ir.aboutcoupang.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=19025871 **(Ex. 01)**.

from only approximately 3,000 accounts.[25] The investigation concluded that the information accessed was limited to names, email addresses, phone numbers, shipping addresses, certain order histories, and building codes to shared spaces where packages could be delivered, and did not include any financial information such as credit card data, Government-issued identification numbers, login credentials, or home entry codes.[26] There is currently no evidence that any of the stolen data was sold, transferred, or shared.[27] The threat actor never made any blackmail or similar threats, and has repeatedly stated that the data never left his control.

Petitioners understand that Coupang worked closely with the Korean Government during its investigation. Coupang reportedly maintained a frequently used and open line of communication with NIS regarding the breach, and closely coordinated with the NIS on its own investigation and efforts to retrieve the stolen data.[28] Acting under NIS instructions, Coupang's legal team contacted the former employee, secured his cooperation, and obtained the relevant devices relating to the data breach—all by December 16, 2025.[29] In short, due to the close collaboration between Coupang and Korean Government officials, the breach was neutralized in less than one month from Coupang's initial discovery. During this time, the NIS requested that Coupang keep the operation confidential, which Coupang did, all while the Government falsely accused Coupang of failing to seriously address the breach.[30] Notwithstanding this cooperation

---

[25] *Id.* at Item 1.05 (Dec. 29, 2025).

[26] *Id.* at Exhibit 99.1.

[27] *Id*.

[28] *Id*.

[29] *Id.*

[30] *Id*.

and containment success, senior officials later publicly disclaimed or contradicted core aspects of the containment effort, further fueling a false narrative.

2. The Korean Government's Response

The response to what was objectively a limited data breach has been entirely disproportionate and unjust. Despite government knowledge of the facts of the breach, in early December, President Lee stated that companies violating data security rules should be hit with fines "so severe that they go out of business" and, in a clear reference to Coupang, asked, "Aren't there some 34 million victims?"[31] In other words, even though there was no evidence that any of the customers affected by the data breach were financially harmed and the breach seems to have been fully contained, President Lee rushed to publicly threaten Coupang's existence. Senior officials also publicly overstated the incident by repeatedly characterizing it as involving tens of millions of "victims" and by implying the compromise of data categories that were not in fact accessed or retained. One official, the Chairperson of the National Policy Committee, went so far as to claim, "[i]t is no exaggeration to say that the personal data of all South Koreans except those under 14 years old have been leaked."[32] But this does appear to have been an exaggeration—and a massive one, by more than four orders of magnitude.

Korean Government agencies quickly fell in line. Despite Coupang's prompt and transparent response, and its close coordination with the NIS, the Korean Government used the

---

[31] Lee Jae Myung, *First-Ever Real-Time Work Report | Ministry of Science and ICT, etc*. (사상 최초, 실시간으로 만나는 업무보고 | 과학기술정보통신부 등), YouTube, at 1:38 (Dec. 11, 2025), https://www.youtube.com/live/WjV9Mq-nKxE?t=5913s.

[32] Lee Mi-ji, *Coupang Founder Indictment Petition Over 33.7M Data Leak*, The Chosun Daily (Dec. 3, 2025), https://www.chosun.com/english/industry-en/2025/12/03/UV7EKGVWS5HMFMI4TIXGVOGYX4/ [https://perma.cc/UB2Y-L6RL] **(Ex. 31)**.

incident as a pretext to accelerate its attacks against Coupang. In the middle of Coupang's ongoing cooperation with the NIS, Korean officials leaked news of the breach to the media and launched an aggressive series of overlapping investigations that bore no reasonable relationship to the actual scope of the data breach, including the following:

- On December 9, 2025, the Seoul Metropolitan Police Agency's ("SMPA") Cyber Investigation Division deployed 17 officers to undertake an eight-day search-and-seizure operation at Coupang's Seoul headquarters.[33]

- On December 11, 2025, President Lee advocated for the creation of a class action system in Korea, so that "when [companies] harm the public, penalties [are] strong enough to make companies fear they could collapse."[34] President Lee also began publicly attacking Coupang outside the context of the data breach, alleging that special regulations were necessary for Coupang because of how badly they overworked their employees, claiming that "[s]ome argue we should ban this . . . Coupang's employment structure . . . seems like a new form of labor requiring new regulatory approaches."[35]

- On December 18, 2025, despite ongoing cooperation with Korean authorities, the Korean Government announced the creation of an inter-ministerial task force focused on the data breach. The agencies involved include the National Police Agency; the PIPC; the Financial Services Commission, a financial regulator that chiefly supervises banks and would not typically participate in an investigation involving neither financial information nor financial institutions; the Korea Media and Communications Commission which, as its name implies, regulates media rather than retail companies; and the NIS.[36] The formation of overlapping, multi-agency task forces—paired with

---

[33] Kukmin Ilbo, *Police Raid Coupang Over "Personal Information Leak" ... Plan to Identify Leaker and Pathway* (Dec. 9, 2025), https://www.kmib.co.kr/article/view.asp?arcid=0029088058&code=61121111&cp=nv [https://perma.cc/92TY-JYS2] **(Ex. 32)**.

Petitioners understand that the investigation was launched under the Personal Information Protection Act. *See* Personal Information Protection Act (Act No. 19234, Mar. 14, 2023) **(Ex. 18)**; Enforcement Decree of the Personal Information Protection Act (Presidential Decree No. 35343, Feb. 25, 2025) **(Ex. 19)**.

[34] Dong-A Ilbo, *Lee Calls for Tougher Fines After Coupang Data Leak* (Dec. 13, 2025), https://www.donga.com/en/article/all/20251213/6009706/1 [https://perma.cc/3L73-4B67] **(Ex. 33)**.

[35] Han Jae-joon & Kim Ji-hyun, *"My Sister Also Died In the Bathroom at Dawn"... President Lee Targets Coupang Over Overwork Deaths*, News 1 Korea (Dec. 11, 2025), https://www.news1.kr/politics/president/6005974 [https://perma.cc/F8Z2-WET2] **(Ex. 34)**.

[36] Kim Kang-han, *Government Forms Cross-Ministerial Task Force to Address Coupang Hacking*, The Chosun Daily (Dec. 18, 2025), https://www.chosun.com/english/industry-en/2025/12/18/V5K7U3BHGJB2LPWY46SAQN5GOY/ [https://perma.cc/SD9W-8ESQ] **(Ex. 35)**.

parallel raids and inspections—reflected an extraordinary mobilization against a single company that far exceeds any rational response to the incident's facts.

- On December 19, 2025, Prime Minister Kim Min-seok urged Government regulators to approach enforcement against Coupang for the data breach "with the same determination used to wipe out mafias."[37]

- On January 21, 2026, PIPC Chairman Song Kyung Hee misrepresented the scope of the data breach, claiming it was "certain" that "the personal information of more than 30 million Coupang members was leaked, and if we add nonmember information (such as delivery addresses and phone numbers of nonmembers like family members entered by subscribers), the scale is likely to grow further."[38]

This was the tip of the iceberg. Korea weaponized its entire state apparatus to apply overwhelming pressure on Coupang through unfounded investigations, threats, and sweeping sanctions, representing a public effort to destroy Coupang's reputation, disrupt its business operations, and ultimately attempt to remove a successful U.S. technology company from the Korean market. These pretextual actions launched one after the other occurred throughout December, and have continued to the present day:

- On December 8, 2025, just nine days after Coupang publicly disclosed the data breach, the KFTC began investigating whether Coupang's membership cancellation process for certain of its services violates the Electronic Commerce Act (the "ECA") as a "dark" or deceptive practice.[39] The KFTC informed Coupang that it was required to submit

---

[37] MBC News, *Coupang, Which has Sparked Nationwide Outrage, Was Mentioned Again by President Lee Jae-myung During his Public Work Report*, YouTube, at 1:22–1:40; 2:11–2:26, https://www.youtube.com/watch?app=desktop&v=MRC5peuNy90&t=180s.

[38] Lee Jae-eun, *Korea privacy chief vows to fight SK Telecom suit and intensify Coupang probe*, Chosun Biz (Jan. 21, 2026), https://biz.chosun.com/en/en-it/2026/01/21/STSOAI6FFZDBPFOMB75GP47AR4/ [https://perma.cc/UJ86-FMAM] **(Ex. 36)**.

[39] Moon Chaeseok, *Fair Trade Commission Investigates Legality of Coupang's Complicated Withdrawal Process... "Correction First, Sanctions Later,"* Asian Business Daily (Dec. 8, 2025), https://cm.asiae.co.kr/en/article/2025120821143583305 [https://perma.cc/ACD9-4D9Z] **(Ex. 37)**.

Petitioners understand that this request was made pursuant to the Act on Consumer Protection in Electronic Commerce and the Act on the Regulation of Terms and Conditions. *See* Act on Consumer Protection in Electronic Commerce (Act No. 20534, Dec. 3, 2024) **(Ex. 38)**; Enforcement Decree of the Act on the Consumer Protection in Electronic Commerce (Presidential Decree No. 35257, Feb. 11, 2025) **(Ex. 39)**; Act on the Regulation of Terms and Conditions (Act No. 20240, Feb. 6, 2024) **(Ex. 40)**; Enforcement Decrees of the Act on the Regulation of Terms and Conditions (Presidential Decree No. 29295, Nov. 20, 2018) **(Ex. 41)**.

measures to change its cancellation process before the KFTC had even determined that the company violated the ECA.[40] The KFTC is also closely reviewing the terms and conditions that govern all of Coupang's services for other possible violations.[41]

- On December 10, 2025, the KFTC conducted on-site work at Coupang's corporate headquarters in Seoul in furtherance of the investigations into Coupang's membership cancellation process and terms of service.[42]

- On December 22, 2025, the National Tax Service ("NTS") organized a 150-member *ad hoc* tax audit task force to target Coupang's operations,[43] even though tax information had nothing to do with the data breach, and the NTS had given Coupang a clean audit the prior year.[44] By way of comparison, in 2025, the NTS created special task forces to uncover high-value tax delinquencies related to nearly $75 billion in unpaid taxes.[45] Those task forces totaled only 56 members.[46] The scope and staffing of this Coupang-specific deployment underscores the retaliatory character of the audit.

---

[40] Moon Chaeseok, *Fair Trade Commission Investigates Legality of Coupang's Complicated Withdrawal Process... "Correction First, Sanctions Later,"* Asian Business Daily (Dec. 8, 2025), https://cm.asiae.co.kr/en/article/2025120821143583305 [https://perma.cc/ACD9-4D9Z] **(Ex. 37)**.

[41] *Id.*

[42] Kim Seung-hyeon, *Korea Fair Trade Commission Probes Coupang's Cancellation Process, Exemption Clauses*, The Chosun Daily (Dec. 10, 2025), https://www.chosun.com/english/market-money-en/2025/12/10/OKQXT2TV4FFQZIQWEITAYASJUY/ [https://perma.cc/UHY6-NJS9] **(Ex. 42)**.

Petitioners understand that these inspections occurred pursuant to the MRFTA, Customs Act, and the Act on the Regulation of Terms and Conditions. *See* Monopoly Regulation and Fair Trade Act (Act No. 20711, Jan. 21, 2025) **(Ex. 27)**; Enforcement Decree of the Monopoly Regulation and Fair Trade Act (Presidential Decree No. 35382, Mar. 12, 2025) **(Ex. 28)**; Customs Act (Act No. 19228, Mar. 4, 2023) **(Ex. 43)**; Act on the Regulation of Terms and Conditions (Act No. 20240, Feb. 6, 2024) **(Ex. 40)**; Enforcement Decree of the Act on the Regulation of Terms and Conditions (Presidential Decree No. 29295, Nov. 20, 2018) **(Ex. 41)**.

[43] Framework Act on National Taxes (Act No. 19926, Dec. 31, 2023) **(Ex. 44)**.

[44] Chosun Ilbo, *Coupang's U.S. Headquarters Transactions Also Under Scrutiny... National Tax Service Launches Comprehensive Tax Investigation* (Dec. 22, 2025), https://www.chosun.com/economy/economy_general/2025/12/22/KNFFX2I7IBDM7J77MDO5ADWUOA/?utm_source=naver&utm_medium=referral&utm_campaign=naver-news [https://perma.cc/TY5G-GPFA] **(Ex. 45)**.

[45] PwC, *Korean Tax Update Samil Commentary* (Nov. 14, 2025), https://www.pwc.com/kr/ko/insights/samil-commentary/samilcommenatry_nov2025_en.pdf [https://perma.cc/CC59-6E5N] **(Ex. 46)**.

[46] *Id.*

- On December 29, 2025, the Korea Customs Service launched an on-site investigation of Coupang's Seoul headquarters related to foreign exchange transactions at Coupang's U.S. headquarters.[47]

- During hearings before the National Assembly on December 30 and 31, 2025, at which Coupang's interim CEO appeared, lawmakers suggested that Coupang should face "severe[] sanction[s],"[48] while another called for the National Pension Service to fully divest its approximately $150 million in Coupang holdings.[49] Meanwhile, multiple lawmakers voted to refer Coupang's executives for criminal prosecution, and the National Assembly threatened to indict Coupang's interim CEO for perjury.[50] These actions included criminal referrals tied to testimony and nonappearance, calls to "kick out" senior executives, and demands for travel bans—measures aimed at coercing individuals and deterring U.S.-based management from operating in Korea.

- On January 2, 2026, the SMPA expanded its role, forming an 86-person task force of its own centered on Coupang.[51] In the recent past, the SMPA had formed far smaller special task forces to address critical national issues—rather than an individually named company—like stock price manipulation (37 to 50 members); widespread

---

[47] Jang Sang-min, *Customs Service Launches On-Site Inspection of Coupang Headquarters… Scrutinizes Foreign Exchange Transactions at U.S. Headquarters*, Munhwa (Dec. 29, 2025), https://www.munhwa.com/article/11557323?ref=naver [https://perma.cc/XFK5-464G] **(Ex. 47)**.

[48] Cheonji Ilbo, *Seo Young-kyo: "Coupang's Personal Information Leakage Must Be Severely Sanctioned and Punished,"* (Nov. 30, 2025), https://www.newscj.com/news/articleView.html?idxno=3346222&utm [https://perma.cc/2KA5-55FP] **(Ex. 48)**; Yoo Seung-ho, Seo Young-kyo: *"Coupang's Personal Information Leak Demands Severe Sanctions and Punishment"*, E Today (Nov. 30, 2025), https://www.etoday.co.kr/news/view/2531036 [https://perma.cc/JY6C-E655] **(Ex. 49)**.

[49] Park So-jeong, *National Pension Service reviews Coupang exclusion after 218.1 billion won investment*, Chosun Biz (Dec. 31, 2025), https://biz.chosun.com/en/en-policy/2025/12/31/M4TPO3B6VVG4HDBXTGEQ5WPFUQ/ [https://perma.cc/4YRW-M4DE] **(Ex. 50)**.

[50] Ryu Jeong-hwa, *National Assembly Oversight Committee files charges against 7 individuals including Coupang's Kim Beom-seok and Rogers... "Suspects of failure to appear and perjury"*, JTBC (Jan. 1, 2026), https://news.jtbc.co.kr/article/NB12277951 [https://perma.cc/9T76-PXN2] **(Ex. 51)**; Choi Hyun-joo, *National Assembly Files Charges Against Coupang's Kim Beom-seok, Rogers, and 5 Others for Failure to Appear and Perjury*, JoongAng Ilbo (Dec. 31, 2025), https://www.joongang.co.kr/article/25394306 [https://perma.cc/DGJ7-JMN8] **(Ex. 52)**; Jang Bokyeong, *Science and ICT Committee to File Charges Against Seven Including Coupang's Bom Kim and Rogers for Violating National Assembly Testimony Act*, Asia Business Daily (Dec. 31, 2025), https://cm.asiae.co.kr/en/article/20251231214135934 96#:~:text=Four%20Including%20Harold%20Rogers%20Face, Assembly%20Testimony%20and%20Appraisal%20Act [https://perma.cc/CL87-4DVM] **(Ex. 53)**.

[51] Park Go-eun, *Police Launch 86-Member Coupang Task Force…Investigating All Issues Including Personal Data Leaks and Industrial Accident Cover-Ups*, Hani (Jan. 2, 2026), https://www.hani.co.kr/arti/society/society_general/1237729.html [https://perma.cc/SM6S-TTZP] **(Ex. 54)**.

kidnapping, detention, and torture by criminal organizations operating in Cambodia (44 members); and cryptocurrency fraud involving millions of dollars (30 members).[52]

- On January 5, 2026, Lee Chan-jin, Governor of the FSS, "warned of a rigorous investigation" into Coupang's interest rates on merchant loans, accusing Coupang of "excessive profit" and "bullying," even though those rates are within legal limits.[53]

- On January 6, 2026, the Ministry of Land, Infrastructure and Transport ("MOLIT") withheld approval for a planned real estate investment in logistics centers that was on track to be approved and was unrelated to the breach.[54] Acknowledging the unusual nature of MOLIT's obstruction, the Director of the Investment Policy Division stated, "We are examining the matter in detail, not considering the typical processing time for business permits."[55]

- On January 6, 2026, the Government created another task force focused on Coupang, this time at MOEL, the labor ministry, to investigate the company using "all possible

---

[52] KBS World, *Gov't Set to Expand Response Team to Stop Stock Manipulation* (Dec. 31, 2025), https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=198515 [https://perma.cc/5SZX-BDFP] **(Ex. 55)**; Byun Seonjin, *Commissioner Park Jeongbo of Seoul Police: "Dedicated Task Force Launched to Investigate Overseas Kidnappings and Detentions"*, Asian Business Daily (Oct. 20, 2025) https://www.asiae.co.kr/en/article/2025102011471033770 [https://perma.cc/H7SS-DCCM] **(Ex. 56)**; Kim & Chang, *Establishment of Joint Investigation Unit to Counter Virtual Asset Crimes* (Sept. 27, 2023), https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=28044 [https://perma.cc/H7KP-UAUG] **(Ex. 57)**.

[53] Park Joon-woo, *Payday Loan Levels... Coupang's "8.9% Annual Interest" High-Interest Loan Controversy*, JTBC News (Jan. 5, 2026), https://news.jtbc.co.kr/article/NB12278496 [https://perma.cc/FB6Q-7KK8] **(Ex. 58)**.

[54] Chosun Ilbo, *Ministry of Land, Infrastructure and Transport Puts Brakes on Coupang's Plan to Raise 1 trillion Won by Selling Logistics Centers* (Jan. 1, 2026), https://www.chosun.com/economy/market_trend/2026/01/06/UAW2CK3GYRDDZPI5ARSY5KSWZY/?utm_source=naver&utm_medium=referral&utm_campaign=naver-news [https://perma.cc/38GE-JZ4E] **(Ex. 59)**.

[55] *Id.*

Petitioners understand that this action was taken pursuant to the Occupational Safety and Health Act (Act No. 20522, Oct. 22, 2024) **(Ex. 60)**; *see also* Enforcement Decree of the Occupational Safety and Health Act (Presidential Decree No. 35597, June. 20, 2025) **(Ex. 61)**.

means."[56] It further promised that any violations would be met with "strict measures."[57]

- On January 13, 2026, the KFTC's Enterprise Group Bureau, Market Surveillance Bureau, and Distribution Agency Bureau dispatched 20 investigators to Coupang's corporate headquarters.[58] By the next day, the KFTC was planning an "unprecedented" two-week on-site investigation of Coupang, deploying a large number of investigators.[59]

- On January 16, 2026, MOEL announced that it would deploy 17 labor inspectors to conduct "an intensive investigation into allegations including illegal dispatch, the creation and management of a blacklist, and operation of a low-performer exit program" at Coupang.[60]

None of these actions was focused on the data breach incident itself. Instead, answering a rallying cry from the President, over a dozen agencies launched investigations and raids targeting Coupang, and interfered with routine transactions and business operations. At the same time, Korea escalated pressure against Coupang's leadership through criminal referrals, threatened

---

[56] Choi Seo-eun, *Ministry of Labor Forms Coupang Labor and Industrial Safety Task Force… "Mobilizing All Possible Means for Comprehensive Investigation"*, KyungHyang (Jan. 6, 2026), https://www.khan.co.kr/article/202601061935001#ENT [https://perma.cc/M6AW-RM6W] **(Ex. 62)**.

Petitioners understand that this action was taken pursuant to the Occupational Safety and Health Act (Act No. 20522, Oct. 22, 2024) **(Ex. 60)**; *see also* Enforcement Decree of the Occupational Safety and Health Act (Presidential Decree No. 35597, June. 20, 2025) **(Ex. 61)**.

[57] Choi Seo-eun, *Ministry of Labor Forms Coupang Labor and Industrial Safety Task Force… "Mobilizing All Possible Means for Comprehensive Investigation"*, KyungHyang (Jan. 6, 2026), https://www.khan.co.kr/article/202601061935001#ENT [https://perma.cc/M6AW-RM6W] **(Ex. 62)**.

[58] Kim Seung-hyeon, *Fair Trade Commission Probes Coupang Chairman's Control Designation* (Jan. 13, 2026), https://www.chosun.com/english/market-money-en/2026/01/13/RZ6ZTJYKXFBC3JSAR2LY5K3P7E/ [https://perma.cc/W5XL-QDLX] **(Ex. 63)**.

[59] Naver, *FTC Deploys Massive Workforce for Two-Week On-Site Inspection of Coupang… "Unprecedented Duration and Scale"* (Jan. 14, 2026), https://n.news.naver.com/mnews/article/449/0000332281?sid=101 [https://perma.cc/HPP8-MARP] **(Ex. 64)**.

[60] Kim Nam-hee, *Ministry of Employment and Labor Launches Labor Inspection Into Coupang Blacklist and Illegal Dispatch Allegations*, KyungHyang (Jan. 16, 2026), https://www.khan.co.kr/en/article/202601161541187 [https://perma.cc/WK8U-EZMA] **(Ex. 65)**; Park So-jeong, *Labor Ministry Launches Inspection Into Coupang Over Alleged Labor Violations*, Chosun Biz (Jan. 16, 2026), https://biz.chosun.com/en/en-policy/2026/01/16/DLS6VCRFGFEIBI5JFAB527NBDA/ [https://perma.cc/QD28-5DNK] **(Ex. 66)**; Lee Dongwoo, *Ministry of Labor Launches Labor Inspection Into Coupang Over Allegations of Illegal Dispatch and Blacklists*, Asia Business Daily (Jan. 16, 2026), https://cm.asiae.co.kr/en/article/2026011614513082832 [https://perma.cc/KE5Q-JAZ8] **(Ex. 67)**.

indictments, and travel-ban advocacy—coercive tactics particularly chilling for U.S. nationals and U.S.-headquartered firms.

The animus senior Korean Government officials publicly displayed towards Coupang, combined with the unreasonable and disproportionate response to Coupang's limited data breach, is an appropriate basis on which to act under Section 301. Section 301 defines "discriminatory" to "include . . . any act, policy, and practice which denies national or most-favored nation treatment to United States goods, service, or investment."[61] "[U]nreasonable" refers to an act, policy, or practice that "while not necessarily in violation of, or inconsistent with, the international legal rights of the United States is otherwise unfair and inequitable."[62] Simply put, despite Coupang's response and resolution of a limited data breach incident in close coordination with government officials, the Korean Government has taken concerted and extraordinary steps to impair the company's operations and attack every aspect of its business. Further, no Korean company dealing with a data breach incident has faced a similar whole-of-government response.

In sum, over the past six weeks, in response to a limited data breach involving 3,000 customer accounts, the Government has marshalled against Coupang the resources of over a dozen different agencies; four separate task forces and teams; scores of investigations, inspections, and raids, most of which have nothing to do with the breach; and numerous Government officials, including officials at the highest levels, have advocated for aggressive and unjustified actions

[61] 19 U.S.C. § 2411(d)(5).

[62] 19 U.S.C. § 2411(d)(3)(A).

against Coupang. These types of efforts threaten to cripple Coupang's business and erode its customer base, as users move to Korean competitors.[63]

The goal of the Korean Government's campaign is clear: to halt Coupang's operations in Korea. Its onslaught of investigations, raids, and inspections have forced Coupang to expend tremendous resources responding to each of them, draining the company of time, energy, and money that would have been much better spent running its business and serving its Korean companies. Approximately 400 Government investigators have been deployed against the company.[64] They have already conducted at least 150 face-to-face meetings and 200 interviews, and made over 1,100 document and other information requests.[65] The sheer number of Government officials stationed at Coupang's headquarters and their continuous demands have been paralyzing. Coupang employees have complained that "there are no remaining conference rooms," they have been "creating various materials" for the Government "for over a month," and they "can't work" because they are "responding to face-to-face interview requests."[66]

This whole-of-government onslaught went well beyond any reasonable response to a data breach. Coupang issued a public statement on December 25, 2025, summarizing the results of its investigation. It noted that the threat customer records stored information from only about 3,000 accounts, and this user data was "subsequently deleted" and "never transferred any of the data to

---

[63] Korea Bizwire, *Coupang Data Breach Triggers Shift in Korea's E-Commerce Landscape*, The Korea Bizwire (Jan. 21, 2026), http://koreabizwire.com/coupang-data-breach-triggers-shift-in-koreas-e-commerce-landscape/342492 [https://perma.cc/4APR-8NGH] **(Ex. 02)**.

[64] Jasmine Choi, *Coupang CEO Rogers, "Professionalism and cooperation for investigation by 400 officials from 11 agencies"*, Business Korea (Jan. 21, 2026), https://www.businesskorea.co.kr/news/articleView.html?idxno=261405 [https://perma.cc/N5JY-TQUW] **(Ex. 68)**.

[65] *Id.*

[66] *Id.*

others."[67] Coupang further noted that "[a]ll devices and hard drives the perpetrator used to leak Coupang user data have been retrieved and secured following verified procedures," and "Coupang has also been cooperating fully with all relevant ongoing government investigations."[68] Later in December 2025, Coupang reported the results of its joint investigation with the NIS to Government authorities and provided an update to potentially affected customers. The Korean Government has disregarded those facts, however, as it launched investigation after investigation, raid after raid, and inspection after inspection into seemingly every aspect of Coupang's operations.

3. Disparate Handling of Data Breaches

The intensity of the Korean Government's response is wholly disconnected from the reality of the situation, and it is completely disproportionate to how the Government has reacted to data incidents at Korean companies and non-U.S. foreign companies, including Chinese businesses. Indeed, Korea's responses to prior data breaches shows how extreme, punitive, and disproportionate its response to Coupang's data breach has been. When multiple Korean-owned companies and other foreign companies experienced cybersecurity breaches that were orders of magnitude greater in scope, none faced punishment on par with Korea's response to the Coupang data breach.

One illustrative case is the discovery in 2024 of a data breach by Kakao Pay, a Korean mobile payment service provider. Kakao Pay's parent Kakao is a Korean competitor of Coupang. While this was a case of data transfer rather than data breach, the scope was massive. Over more than six years, Kakao Pay had deliberately transferred 54 billion personal data records of over 40

---

[67] Coupang, *Coupang Has Identified the Leaker and Confirmed that All Devices Used in the Customer Information Leak Have Been Recovered* (Dec. 25, 2025), https://news.coupang.com/archives/58892/ [https://perma.cc/MP79-YXYP] **(Ex. 69)**.

[68] *Id.*

million Korean users to Alipay Singapore, contrary to Korean law.[69] Transferred records included sensitive financial information such as phone numbers, account balances, transaction histories, and credit information. Alipay Singapore is owned by Ant Group, a Chinese affiliate of the Chinese conglomerate Alibaba Group Holding ("Alibaba"). This was not an accidental transfer; it was a deliberate, corporate policy. Yet rather than facing sweeping investigations, public threats, or huge fines, Kakao Pay received approximately $15 million in combined fines, and its CEO received only a "formal warning" that led to neither his dismissal nor criminal prosecution.[70]

Another example that underscores the discriminatory treatment Coupang faces as a U.S. company involves SK Telecom ("SKT"), Korea's largest wireless carrier. In April 2025, SKT experienced a massive cyberattack involving SIM card data from 23 to 27 million customers—the company's entire user base.[71] This represents a breach of the data of more than 7,000 times the number of customers whose data was downloaded in the Coupang incident. And yet, the Korean Government imposed a fine against SKT of $91 million, more than eight times smaller than the

---

[69] Kim Min-Young, *Kakao Pay Under Investigation for Allegedly Leaking 54 Billion Personal Data Entries to China's Alipay*, Korea JoongAng Daily (Sept. 5, 2024), https://koreajoongangdaily.joins.com/news/2024-09-05/national/socialAffairs/Kakao-Pay-under-investigation-for-allegedly-leaking-54-billion-personal-data-entries-to-Chinas-Alipay/2128287 [https://perma.cc/HMQ6-8J98] **(Ex. 70)**.

[70] Yun Ye-won, *Kakao Pay and Apple Fined 8.3 Billion Won for Sharing User Data Without Consent*, ChosunBiz (Jan. 23, 2025), https://biz.chosun.com/en/en-it/2025/01/23/DW5GK2KIVBDQXHUOYIDEOYE6HA/ [https://perma.cc/8TSF-GKC8] **(Ex. 71)**; Park Boram, *Kakao Fined Record 15.1 Bln Won for Leak of Open Chat Users' Personal Data*, Yonhap News Agency (May 23, 2024), https://en.yna.co.kr/view/AEN20240523004900315 [https://perma.cc/L88P-4TUX] **(Ex. 72)**.

[71] *See, e.g.*, KBS World, *SK Telecom Files Administrative Suit Challenging Record Fines Over Data Breach* (Jan. 19, 2026), https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=198937 [https://perma.cc/9QTD-ZAFM] **(Ex. 73)**; Reuters, *South Korea Agency Fines SK Telecom $97 million Over Major Data Leak* (Aug. 28, 2025), https://www.reuters.com/sustainability/boards-policy-regulation/south-korea-agency-fines-sk-telecom-97-million-over-major-data-leak-2025-08-28/ **(Ex. 74)**.

fine President Lee hoped to impose on Coupang.[72] Nor does SKT appear to have faced a whole-of-government effort to disrupt its business, criminal referrals of its executives, or calls from leading politicians for its collapse and bankruptcy.

The Upbit Crypto data security breach, also in November 2025, provides another stark contrast to Korea's response to a data breach by a U.S. company. Upbit is Korea's largest crypto exchange and was acquired by Naver (an internet portal akin to Google in the United States that also includes an e-commerce platform that competes with Coupang) in September 2025.[73] In a hack attributed to North Korea's Lazarus Group, hackers stole over $30 million in victims' crypto assets from Upbit through unauthorized withdrawals, and the hack potentially exposed user data.[74] In response, the police issued a formal probe, the FSS issued warnings for "serious" security failures, the Korean Government began investigating Upbit reporting delays, and the National Assembly considered legislation to strengthen regulations of crypto exchanges.[75] Critically, however, the response stopped there. Unlike Coupang, Upbit has not faced a whole-of-government mobilization resulting in investigations, threats from government officials to put the company out of business, or criminal allegations against senior executives.

---

[72] *See, e.g.*, KBS World, *SK Telecom Files Administrative Suit Challenging Record Fines Over Data Breach* (Jan. 19, 2026), https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=198937 [https://perma.cc/9QTD-ZAFM] **(Ex. 73)**.

[73] Reuters, *Naver's Payment Arm to Acquire South Korean Crypto Exchange Operator in $10 bln Deal* (Nov. 27, 2025), https://www.reuters.com/world/asia-pacific/navers-payment-arm-acquire-south-korean-crypto-exchange-operator-10-bln-deal-2025-11-27/ **(Ex. 74)**.

[74] Omkar Godbole, AI Boost, *South Korea Suspects North Korea-Linked Lazarus Behind $36M Upbit Hack*, Coin Desk (Nov. 28, 2025), https://www.coindesk.com/markets/2025/11/28/south-korea-suspects-north-korea-linked-lazarus-behind-usd36m-upbit-hack **(Ex. 76)**.

[75] Im Eun-byel, *FSS Chief Puts Upbit on Notice Over 'Serious' Security Failures*, The Korea Herald (Dec. 1, 2025), https://www.koreaherald.com/article/10627202 [https://perma.cc/HND4-FPT2] **(Ex. 77)**.

Finally, just this past week, it was belatedly revealed that the Chinese e-commerce platform AliExpress, another subsidiary of Alibaba, suffered a hack in October 2025 involving highly sensitive information that resulted in the theft of approximately $6 million.[76] AliExpress conducted an internal investigation, but reportedly submitted false statements to Government officials.[77] And yet, the Government response seems to have been limited to the tepid request that AliExpress "prevent recurrence" of these types of hacks in the future.[78]

This stark disparity between Korea's response to Coupang and its treatment of data incidents at Kakao Pay, Upbit, SK Telecom, and AliExpress underscores the Korean Government's discriminatory targeting of a successful U.S. technology company. Coupang, a U.S.-owned company, has been singled out for punitive treatment—indeed, for it to "collapse"[79] or be "wipe[d] out"[80]—wholly inconsistent with Korea's treatment of more-serious data incidents involving Korean-owned or Chinese-owned companies.

The facts and government statements speak for themselves. The Korean Government's continued escalation against Coupang shows that Coupang is not facing isolated enforcement

---

[76] Lee Joo-bin, *AliExpress "Seller Account" Hacked, 8.6 Billion Won Stolen... "Police Report" Was a Lie Too*. Hani (Jan. 19, 2026), https://www.hani.co.kr/arti/economy/economy_general/1240535.html [https://perma.cc/G93T-57WU] **(Ex. 78)**.

[77] *Id.*

[78] *Id.*

[79] Kim Tae-jun, *Exclusive: Presidential Office Prohibits Staff From Contacting Coupang*, The Chosun Daily (last updated Dec. 25, 2025), https://www.chosun.com/english/national-en/2025/12/25/RRXZA7V2EJBGZJHRZBZO7N7BL4/ [https://perma.cc/NY3C-5BKF] **(Ex. 03)**; The Dong-A Ilbo, *Lee calls for tougher fines after Coupang data leak* (Dec. 13, 2025), https://www.donga.com/en/article/all/20251213/6009706/1 [https://perma.cc/3L73-4B67] **(Ex. 33)**.

[80] MBC News, *Coupang, which has sparked nationwide outrage, was mentioned again by President Lee Jae-myung during his public work report*, YouTube, at 1:22–1:40; 2:11–2:26, https://www.youtube.com/watch?app=desktop&v=MRC5peuNy90&t=180s.

actions, but a coordinated campaign of state pressure that continues to grow in scope, severity, and coercive effect. Korean lawmakers appear to recognize the trade implications of their discriminatory conduct, but at the same time believe they will not be sanctioned. As one Korean lawmaker suggested, "U.S. authorities, such as the U.S. Trade Representative, have not issued any official messages on Coupang, so Korea does not have to care much for any possible trade risk with the U.S. due to the latest incident."[81] That should change.

IV. REQUESTED COUNTERMEASURES

To address Korea's unreasonable and discriminatory acts against Coupang, which burden and restrict U.S. commerce, Petitioners request (1) the imposition of tariffs on certain Korean goods entering the United States as well as the imposition of licensing and/or other restrictions on Korean services in the United States; (2) negotiation of more-detailed protections and nondiscriminatory-treatment provisions to prevent the Korean Government from abusing its investigatory and enforcement authority to target U.S. firms unreasonably, building on the important commitments set out in the 2025 U.S.-Korea Trade Framework Agreement or as part of a separate agreement; and (3) any additional remedy USTR deems appropriate under the circumstances. In combination, these remedies will incentivize the Korean Government to eliminate the acts, policies, and practices documented in this petition and to ensure a level playing field for not only Coupang but also all U.S. companies and investors operating in Korea.

---

[81] Lee Min-hyung, *Coupang's US Lobby Can't Block Korean Sanctions: Lawmaker*, The Korea Times (Dec. 30, 2025), https://www.koreatimes.co.kr/business/companies/20251231/coupangs-us-lobby-cant-prevent-korean-sanctions-lawmaker [https://perma.cc/A8R6-RNDG] **(Ex. 79)**.

A. Tariffs on Korean Goods Entering the United States and Restrictions on Korean Services

Under Section 301(c)(1)(B), USTR is authorized to impose tariffs and restrictions on services without regard to whether the goods were involved in the act, policy, or practice that is the subject of the action.[82] The Trump Administration has had significant success in using tariffs as a policy tool to address unfair and discriminatory practices by other countries, leading to a record decrease in the U.S. trade deficit, and to increasingly fair terms of trade and commercial opportunities for U.S. companies operating abroad. And the Administration recently warned the Korean Government of a potential Section 301 investigation if it engaged in further discriminatory treatment of U.S. firms.[83] The commitments secured in the recent 2025 U.S.-Korea Trade Framework Agreement reflects the effective use of this approach. As the recent whole-of-government attack on Coupang shows, however, additional action is required to ensure a level playing field for U.S. companies in Korea. USTR should therefore use its broad Section 301 authority to impose additional tariffs on Korean goods and restrictions on Korean services to incentivize the country to address the type of specific, ongoing discrimination and unreasonable treatment that U.S. companies, and Coupang in particular, continue to endure.

B. Detailed Protections and Nondiscriminatory-Treatment Commitments

Korean Government agencies have a history of selective and aggressive enforcement. And despite Korea's recent commitment under the U.S-Korea Trade Framework Agreement "to ensure that U.S. companies are not discriminated against and do not face unnecessary barriers in terms of

---

[82] 19 U.S.C. § 2411(c)(1)(B).

[83] Ari Hawkins, *Trump admin to S Korea: We'll launch trade investigation if you pursue digital regulations*, Politico Pro (Nov. 19, 2025), https://subscriber.politicopro.com/article/2025/11/trump-admin-to-s-korea-well-launch-trade-investigation-if-you-pursue-digital-regulations-00658813 [https://perma.cc/MQ8A-VZT9] **(Ex. 80)**.

laws and policies concerning digital services," the Government's unreasonable treatment of Coupang demonstrates that it flouts this broad commitment in favor of further discriminatory and unreasonable conduct aimed at U.S. interests. Attacking successful U.S. companies in this way constitutes a serious burden on U.S. commerce, as U.S. industry has to spend valuable resources defending itself against spurious charges, investigations, and punitive measures, rather than focusing on technological innovation, growth, and job creation.

USTR should continue its efforts to correct this market handicap by using its authority under Section 301(c) to secure further commitments from Korea regarding nondiscriminatory treatment and impartial administration of its laws, regulations, and investigations. Korea also should be required to guarantee due process in all enforcement proceedings by providing companies with notification of investigations, access to information that is necessary and relevant to any defense to the investigation, rights to legal counsel, and the opportunity to meaningfully contest allegations before an impartial adjudicator. Given Korea's history of unfounded and discriminatory use of competition law and regulatory enforcement tools to constrain Coupang and other successful U.S. technology companies and unfairly protect domestic competitors, USTR should seek a detailed commitment to prohibit such abuse. Cloaking aggressive anti-competitive conduct by the Korean Government under the guise of competition law must come to an end once and for all.

V. PUBLIC HEARING AND OTHER FORMS OF RELIEF

Petitioners request that USTR hold a public hearing regarding this petition, consistent with 19 U.S.C. § 2412(a)(4). Petitioners have not filed and do not currently plan to file for other forms of relief under the Trade Act of 1974. Separately, Greenoaks and Altimeter intend to serve a notice

of intent to bring arbitration claims against the Korean Government for violations of the investment provisions of the U.S.-Korea Free Trade Agreement. Those claims are not the subject of this petition. Rather, Petitioners believe that a separate remedy under Section 301 remains necessary and appropriate to address the burdens on U.S. commerce resulting from Korea's unreasonable and discriminatory conduct against Coupang.

VI. CONCLUSION

The Korean Government's illegal actions toward Coupang have already had material economic consequences for Petitioners and other U.S. investors. Coupang's share price has declined as a direct result of the Korean Government's unjustified response to a limited data breach; equity analysts have issued downgrades; U.S. class actions and related proceedings have multiplied; and Coupang's domestic competitors have exploited the situation.

Coupang is currently facing a whole-of-government assault on its business in Korea, with the President of Korea making his desire to bankrupt the company well-known. The pattern of increasingly severe, unreasonable, and discriminatory treatment by the Korean government that has followed must be checked; aggressive government action to bankrupt a U.S. company and force it out of a foreign market should not be tolerated. Petitioners therefore request that USTR promptly initiate an investigation under Section 301 and adopt urgent countermeasures.

Respectfully submitted,

Marney L. Cheek
Kathleen McNulty
John Catalfamo
Julia Shults
COVINGTON & BURLING LLP
One CityCenter 850 Tenth Street, N.W.
Washington, DC 20001-4956
Tel: +1 (202) 662 5267 | mcheek@cov.com

Counsel to Greenoaks
Capital Partners LLC and
Altimeter Capital Management, LP