HOUSE JUDICIARY COMMITTEE

Chairman Jim Jordan

CLOSED FOR COMPETITION: SOUTH KOREA'S DISCRIMINATORY ATTACKS ON AMERICAN-OWNED BUSINESSES

Interim Staff Report

Committee on the Judiciary
Chairman Jim Jordan

Subcommittee on the Administrative State, Regulatory Reform, and Antitrust
Chairman Scott Fitzgerald

U.S. House of Representatives

July 1, 2026

EXECUTIVE SUMMARY

The Committee on the Judiciary has jurisdiction over the "[p]rotection of trade and commerce against unlawful restraints and monopolies."[1] On February 5, 2026, the Committee and its Subcommittee on the Administrative State, Regulatory Reform, and Antitrust opened an investigation into efforts by the South Korean government to target innovative American-owned companies and subject them to punitive obligations, excessive fines, and discriminatory enforcement practices for the purpose of protecting their South Korean rivals from competition.[2] As part of this investigation, the Committee and Subcommittee issued a subpoena compelling Coupang Inc., an American-owned ecommerce company operating in South Korea, to produce documents and communications related to South Korea's discriminatory attacks on American-owned companies.[3] The subpoena also required Coupang's General Counsel and Chief Administrative Officer, Harold L. Rogers, to participate in a deposition.[4] Through this oversight, the Committee and Subcommittee have uncovered evidence that the South Korean government has engaged in discriminatory attacks on American businesses.

While South Korea has been targeting American-owned companies for decades, its discriminatory treatment has escalated considerably in recent years. Both deposition testimony and documents produced to the Committee and Subcommittee show that:

- South Korea has a long history of engaging in economic discrimination against foreign companies. In the early 2000s, U.S. officials noted their concerns about the fact "that Seoul *continues* to use government regulations and standard-setting powers to *discriminate against foreign firms* in politically sensitive industries."[5] Members of Congress were already discussing then the "longstanding harmful practices of the Korean government to discriminate against [American] products in their domestic market."[6] These practices include coercive investigation tactics, overly burdensome regulatory requirements, and massive fines and penalties intended to punish American companies and make it harder for them to effectively compete against Korean companies.[7]

- While the South Korean government uses every regulatory tool at its disposal to target foreign companies, the Korea Fair Trade Commission (KFTC) has been particularly aggressive in its attacks on American-owned businesses.[8] In a recent survey, American businesses reported that KFTC enforcement is characterized by a "[l]ack of due process

[1] Rules of the House of Representatives R. X (2025).
[2] *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary to Mr. Harold L. Rogers, Chief Administrative Officer and General Counsel, Coupang, Inc. (Feb. 5, 2026).
[3] *Id.*
[4] *Id.*
[5] MARK E. MANYIN, CONG. RSCH. SERV., RL30566, SOUTH KOREA-U.S. ECONOMIC RELATIONS: COOPERATION, FRICTION, AND PROSPECTS FOR A FREE TRADE AGREEMENT (FTA) (2006), at 12-13 (emphasis added).
[6] *The U.S.-Korea Free Trade Agreement Negotiations*, *Hearing Before the Subcomm. Trade of the H. Comm. on Ways and Means*, 110th Cong. (2007) (hereinafter "U.S.-Korea Free Trade Agreement Hearing").
[7] *See infra* Sections I.A, I.B, II.A.
[8] *See* CPNG-HJC119-0000421; CPNG-HJC119-0001715; CPNG-HJC119-0001706; *U.S. Chamber of Commerce Comments on Unfair Trade Practices*, U.S. CHAMBER OF COMMERCE (Mar. 12, 2025).

and procedural fairness,"[9] including the initiation of investigations based on insufficient evidence and the inability of companies to challenge investigations before a final determination is reached by the agency.[10] Even worse, the KFTC regularly uses aggressive enforcement practices in order to coerce compliance, including early morning raids, multi-day interrogations, and even the threat of criminal charges.[11]

- South Korea has weaponized digital laws and regulations to hinder the ability of innovative American companies to effectively compete in its market.[12] The South Korean government is currently advancing legislation modeled directly on the Digital Markets Act (DMA), a European law specifically designed to hinder the ability of American-owned businesses to compete against their European rivals.[13] It has also used overly prohibitive app store restrictions and burdensome cloud service provider requirements as a tool to prevent American companies from successfully competing against Korean digital service providers.[14]

- As part of its broader pattern of economic discrimination, South Korea has engaged in a harassment campaign against Coupang Inc. and its South Korean subsidiary Coupang Corp. (collectively, "Coupang").[15] South Korean regulators have consistently targeted Coupang and subjected the company to hostile regulatory treatment, unfair enforcement practices, and disproportionately large penalties not faced by their Korean competitors.[16]

- After a disgruntled former employee recently accessed Coupang's data systems without authorization, South Korea escalated its attacks into a "whole-of-government assault on Coupang."[17] South Korean officials have repeatedly spread false information about the

[9] CPNG-HJC119-0000421, at 423.
[10] *See id.* at 423-25.
[11] *See id.* at 425.
[12] *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary to Mr. Han Ki-jeong, Chairman, Korea Fair Trade Commission (July 24, 2025) (hereinafter "July 24 Letter"); CPNG-HJC119-0001715; Charles Freeman, *U.S. Chamber Warns Against Rush to Pass Korea's Online Platform Competition Promotion Act; Calls for Transparency and Dialogue*, CHAMBER OF COMMERCE (Jan. 29, 2024); Lilla Nóra Kiss, *Will Korea Burn Its Digital Future Down?*, ITIF (Jun. 12, 2024); Lilla Nóra Kiss, *Why South Korea Should Resist New Digital Platform Laws*, ITIF (Dec. 9, 2024).
[13] *See* Kiss, *Will Korea Burn Its Digital Future Down?*, *supra* note 12; Lilla Nóra Kiss, *Why South Korea Should Resist New Digital Platform Laws*, *supra* note 12; Javier Espinoza, *EU should focus on top 5 tech companies, says leading MEP*, FINANCIAL TIMES (May 30, 2021); Dita Charanzová, *Turning Europe's internet into a 'walled garden' is the wrong path to take*, FINANCIAL TIMES (Feb. 17, 2021); *Europe is now a corporate also-ran. Can it recover its footing?*, THE ECONOMIST (Jun. 5, 2021).
[14] *See* Ella Geris, *South Korea passes 'anti-Google law'*, JURIST (Sept. 2, 2021); CPNG-HJC119-0000001, at 259; *South Korea's Cloud Service Restrictions*, ITIF (Feb. 5, 2026); *Comments of the Computer & Communications Industry Association Regarding Foreign Trade Barriers to U.S. Exports for 2025 Reporting*, CCIA (Oct. 17, 2024), at 168.
[15] *See* CPNG-HJC119-0000421; Yonhap, *US lawmaker accuses Korean regulators of 'discriminatory' actions against Coupang*, KOREA TIMES (Jan. 14, 2026); Deposition of Mr. Harold L. Rogers, Chief Administrative Officer and General Counsel, Coupang Inc., Acting Chief Executive Officer, Coupang Corp. (Feb. 23, 2026).
[16] *See* CPNG-HJC119-0000421; Yonhap, *supra* note 15; Deposition of Mr. Harold L. Rogers, *supra* note 15.
[17] CPNG-HJC119-0001673, at 1675; Yonhap, *supra* note 15; *Spy agency requests Natl Assembly to charge Coupang chief over alleged perjury*, KOREA HERALD (Dec. 31, 2025); Yonhap, *FTC chief says business suspension of Coupang possible amid data-breach probe*, KOREA TIMES (Jan. 12, 2026); Deposition of Mr. Harold L. Rogers, *supra* note 15.

incident, called for the suspension of Coupang's business operations, and referred to Coupang as a criminal organization.[18] Over ten different South Korean agencies have initiated dozens of unrelated investigations into Coupang following the former employee's unauthorized access, issuing over 4,000 document requests and conducting at least 652 interviews with Coupang employees.[19] South Korea's National Intelligence Service (NIS) forced Coupang to send an employee to China in order to recover devices and sworn statements related to the data incident.[20] NIS then lied to the public about its involvement in the recovery operation.[21] Even more concerning, the South Korean government is now threatening Coupang's interim CEO Harold L. Rogers, an American citizen, with criminal charges based on NIS's refusal to acknowledge its role in the recovery operation.[22]

- Following South Korea's campaign against the company, Coupang's market capitalization has fallen by more than 40 percent.[23] This decrease negatively affects U.S. investors, including public pension funds, mutual funds, and everyday Americans saving for retirement.[24] The South Korean government's attacks on Coupang have also harmed other American businesses, which sell billions of dollars' worth of products through Coupang's online platform every year.[25] On June 11, 2026, South Korea fined Coupang over $410 million, the largest fine ever imposed on a single company that far exceeds fines imposed on South Korean companies for more serious data breaches involving highly sensitive personal information.[26] Beyond Coupang, recent estimates indicate that South Korea' discriminatory behavior could lead to over $500 billion in economic losses for the United States and cost the average American household $3,800 over the next 10 years.[27]

South Korea's discriminatory treatment of American-owned businesses directly violates its recent trade agreement with the United States.[28] The Trump Administration has explicitly warned that it will not tolerate foreign efforts to engage in regulatory practices "that are more burdensome and restrictive on United States companies than their own domestic companies."[29] The Committee on the Judiciary has previously raised concerns about South Korea's economic

[18] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 77, 128-40; CPNG-HJC119-0000455; CPNG-HJC119-0000631; CPNG-HJC119-0001597, at 1604-07; CPNG-HJC119-0001709.
[19] *See* CPNG-HJC119-0001994.
[20] *See* CPNG-HJC119-0000887; CPNG-HJC119-0001070; CPNG-HJC119-0001549; CPNG-HJC119-0002057.
[21] *See* CPNG-HJC119-0000887; CPNG-HJC119-0001070; CPNG-HJC119-0001549; CPNG-HJC119-0002057.
[22] *See* CPNG-HJC119-0000876, at 876-77; CPNG-HJC119-0001065, at 1065-66; CPNG-HJC119-0000440, at 440-54.
[23] *See Coupang, Inc. (CPNG)*, YAHOO FINANCE (last visited May 20, 2026).
[24] *See* CPNG-HJC119-0001673; *U.S. investment firms take legal action against South Korea over Coupang*, INVESTING (Jan. 22, 2026).
[25] *See* CPNG-HJC119-0001673, at 1680.
[26] Kwanwoo Jun, *South Korea Fines Coupang $410 Million Over Data-Law Breaches*, WALL STREET JOURNAL (June 11, 2026); Lee Gyu-lee, *Coupang's record privacy fine sparks proportionality debate, investment concerns*, KOREA TIMES (Jan. 12, 2026).
[27] Alden Abbott, *How Korean Antitrust Lawsuits Are Changing U.S. Regulatory Norms*, FORBES (Nov. 4, 2025).
[28] *See* WHITE HOUSE, JOINT FACT SHEET ON PRESIDENT DONALD J. TRUMP'S MEETING WITH PRESIDENT LEE JAE MYUNG (Nov. 13, 2025).
[29] WHITE HOUSE, DEFENDING AMERICAN COMPANIES AND INNOVATORS FROM OVERSEAS EXTORTION AND UNFAIR FINES AND PENALTIES (Feb. 21, 2025).

discrimination against American companies, as have various government officials and members of Congress.[30] This report provides additional evidence of South Korea's discriminatory behavior and the ways in which it has escalated over the past several years. South Korea's economic discrimination against American-owned businesses is part of a larger pattern of foreign governments weaponizing their broad discretion under competition laws and other regulatory regimes to shield their domestic industries from U.S. competition. The Committee and Subcommittee will continue to conduct oversight of these foreign anti-competitive regimes to inform potential legislative reforms to protect American businesses and consumers.

[30] *See* July 24 Letter, *supra* note 12; CPNG-HJC119-0000398; CPNG-HJC119-0000404; CPNG-HJC119-0000405; Letter from Rep. Carol Miller et al. to Hon. Jamieson Greer, United States Trade Representative (Mar. 3, 2026); Kim Eun-joong, *U.S. Lawmakers Demand South Korea Drop Cloud Barriers*, CHOSUN DAILY (Mar. 6, 2026); Yoon Ju-heon, *U.S. Vice President JD Vance Warns South Korea Against Targeting American Tech Companies*, CHOSUN DAILY (Jan. 28, 2026).

TABLE OF CONTENTS

I. SOUTH KOREA DISCRIMINATES AGAINST AMERICAN-OWNED BUSINESSES

For decades, South Korea has weaponized its government agencies to attack American-owned businesses in order to protect Korean companies from competition.[31] As part of this effort, South Korea regularly uses coercive enforcement practices, burdensome regulatory obligations, and excessively large fines to punish American companies and increase their compliance costs.[32] Even worse, South Korea goes as far as to subject executives of American companies to criminal charges, travel restrictions, and even the threat of imprisonment for commonplace regulatory violations, a pattern that is often motivated by political considerations rather than legitimate law enforcement objectives.[33] This discrimination has created a regulatory environment in South Korea that punishes foreign investment and is overtly hostile to American-owned businesses.[34]

While South Korean economic discrimination occurs across various government agencies and sectors of the economy, the KFTC has been particularly aggressive in using competition policy to attack American companies. The KFTC regularly violates due process by initiating investigations based on very little evidence without giving companies the ability to challenge the grounds on which the investigation is based.[35] Even more troubling, unlike most competition enforcement authorities, the KFTC is empowered to bring criminal charges for almost any regulatory violation, and has shown an increased willingness to do so over the past several years.[36] Similarly, South Korea has used digital laws and regulations as a way to target American companies and limit their ability to operate successfully in South Korea.[37]

The South Korean government's discriminatory targeting of American-owned businesses is not just a problem for U.S. companies, but for consumers as well. Based on recent estimates, South Korea's discriminatory enforcement practices and hostile regulatory environment could "lead to [economic] losses of up to $469 billion for Korea and $525 billion for the United States" and "cost the average U.S. household roughly $3,800 in economic losses over the next 10 years."[38] While the cost of South Korea's economic discrimination falls most directly on the businesses that it has decided to target, it is consumers from both the United States and South Korea that will ultimately be harmed by the South Korean government's anticompetitive attacks on American companies.[39]

[31] *See infra* Section I.A.
[32] *See infra* Sections I.A, I.B, II.A.
[33] *See* U.S. Chamber of Commerce, *supra* note 8.
[34] *See* CPNG-HJC119-0000421; CPNG-HJC119-0001673.
[35] *See* CPNG-HJC119-0000421, at 423-24.
[36] *See id.* at 426; Sangyun Lee, *Duplicate Powers in the Criminal Referral Process and the Overlapping Enforcement of the Competition and Criminal Authorities in Korea: An Analysis Through the Lens of the Redundancy Theory*, 519 HUM. RTS. & JUST. 31 (2024).
[37] *See* July 24 Letter, *supra* note 12; CPNG-HJC119-0001715; Kiss, *Will Korea Burn Its Digital Future Down?*, *supra* note 12; CCIA, *supra* note 14, at 168.
[38] Abbott, *supra* note 27.
[39] *See id.*

A. South Korea Has a Long History of Discriminating against Foreign Companies

South Korea has a long and well-documented history of engaging in economic discrimination against American-owned companies and other foreign businesses. A recent United States Trade Representative (USTR) petition explains that "[t]here is no shortage of examples of the Korean Government targeting U.S. companies with overly aggressive enforcement actions."[40] "In Korea," according to business groups, "U.S. companies face an opaque regulatory framework that at times fails to measure up to internationally recognized good regulatory practices," where laws and regulations are often "crafted behind the scenes" in order "to benefit domestic interests at the expense of foreign competitors."[41]

South Korea's hostile approach to foreign competitors is not a new phenomenon. In 2004, Eun Sup Lee, a Professor of International Trade Law and Practice at Pusan National University in South Korea, wrote an article highlighting how "the Korean government has been criticized for . . . maintaining regulatory systems" that "give[] governmental officials room to exercise wide discretion in applying those laws and regulations, resulting in inconsistency in their application and uncertainty in doing business in Korea."[42] Similarly, a Congressional Research Service report from 2006 on economic relations between the United States and South Korea noted that "[m]any U.S. government officials . . . complain that Seoul *continues* to use government regulations and standard-setting powers to *discriminate against foreign firms* in politically sensitive industries."[43]

In a 2007 congressional hearing before the House Committee on Ways and Means' Subcommittee on Trade, then-Chairman Sander M. Levin emphasized the "*longstanding* harmful practices of the Korean government to discriminate against [American] products in their domestic market."[44] In his words, the "two previous Korean commitments" to address these discriminatory practices "were not worth the paper they were written on."[45] The ineffectiveness of these previous efforts to address discriminatory practices resulted, in part, from the fact that the South Korean government "clings to its persistent denial that there has been a government policy to shelter its market, a denial that flies in the face of facts on the ground *over the decades*."[46] Similarly, then-Ranking Member Walter Herger condemned South Korea's "opaque and discriminatory regulatory process" that had worked to "effectively foreclose market access for [American] companies."[47]

In sworn testimony before the Trade Subcommittee, Ford Motor Company's Vice President of International Governmental Affairs, Stephen E. Biegun, explained that South Korea's discriminatory enforcement practices prevented Ford from meaningfully competing

---

[40] CPNG-HJC119-0001673, at 1681.
[41] U.S. Chamber of Commerce, *supra* note 6.
[42] Eun Sup Lee, *Anti-Competitive Practices as Trade Barriers used by Korea and Japan: Focusing on Service and Investment Markets*, 16 BOND L. REV. 117, 141 (2004).
[43] Manyin, *supra* note 5, at 12-13 (emphasis added).
[44] U.S.-Korea Free Trade Agreement Hearing, *supra* note 6 (emphasis added).
[45] *Id.*
[46] *Id.* (emphasis added).
[47] *Id.*

against Korean car manufacturers.[48] He testified that "Ford's lack of access into the Korean market" was the direct result of "an elaborate layering and ever changing presence of non-tariff barriers that work effectively to block [Ford's] products."[49] Mr. Biegun analogized South Korea's discriminatory treatment to "the old arcade game Wac-A-Mole," where "[n]ew regulations pop up each time we whack one down."[50] Mr. Biegun made it clear that South Korea's economic discrimination was by no means limited to Ford:

> [I]t's important to note that [Ford] [is] not alone. Let me emphasize this point. No manufacturer from any country can make significant sales into the Korean market, not Ford, not General Motors, not Toyota, not Volkswagen, nobody can get significant vehicles into this market.[51]

While South Korea's discriminatory approach to economic regulation has received considerable attention from U.S. lawmakers and government officials in recent months,[52] it has been going on for decades. Researchers, executive branch officials, Members of Congress, and American businesses across different industries have each arrived at the same conclusion: South Korea's regulatory system is intentionally designed to disadvantage foreign competitors and protect Korean companies.[53] The specific enforcement mechanisms used by the South Korean government vary by sector, but the underlying policy of economic discrimination remains the same throughout.

B. South Korea Weaponizes Competition Law to Attack American Businesses

The KFTC's enforcement practices serve as one of the most well-documented examples of how South Korea has weaponized its regulatory agencies and bureaucratic processes against American companies. The KFTC is the South Korean regulatory authority charged with promoting economic competition and protecting consumers from unfair trade practices.[54] However, far from promoting "fair and free competition in the market,"[55] the KFTC regularly engages in "arbitrary investigations, rulings, and actions, which often disproportionately target U.S. companies."[56] As antitrust and competition expert Joseph Coniglio explains, "the facts present a rather clear picture of the KFTC engaging in de facto discrimination against American firms, particularly through large fines or other heavy burdens, including with respect to due process."[57]

---

[48] *See id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *See* CPNG-HJC119-0000398; CPNG-HJC119-0000405; Letter from Rep. Carol Miller et al. to Hon. Jamieson Greer, United States Trade Representative (Mar. 3, 2026).
[53] *See* CPNG-HJC119-0001673, at 1678.
[54] *See Who we are*, Korea Fair Trade Commission (last visited Apr. 30, 2026).
[55] *Id.*
[56] U.S. Chamber of Commerce, *supra* note 8.
[57] CPNG-HJC119-0001706.

According to the National Bureau of Asian Research (NBR), a nonprofit research group, the KFTC "stands out for the scale and nature of its enforcement actions against U.S. firms . . . [e]ven when compared with other active regulators, such as the EU Directorate-General for Competition."[58] In the words of Alden Abbott, the former General Counsel of the Federal Trade Commission, South Korea's "[a]ntitrust cases and planned regulation directed at U.S. companies stem from Korean officials' claims that American firms have an unfair advantage over Korean businesses."[59] This has created an overall environment that is "unpredictable, politicized, and tilted against" American businesses.[60]

For example, in September 2021, the KFTC fined American-owned Google ₩207 billion (approximately $176.6 million) for not allowing device manufacturers like Samsung and LG, two Korean companies that compete directly with Google, to use altered versions of Google's Android operating system.[61] This was the third-largest fine that the KFTC had ever issued against a company for allegedly abusing their dominant status in the market and was "roughly equal to that issued across 4 Samsung companies in 2021 and about two-thirds of the penalty charged that same year to 11 predominantly Korean firms for far more egregious cartel behavior in the steel industry."[62] The two largest fines that the KFTC ever issued for abuse of market dominance were both against Qualcomm, another American-owned company.[63]

Like South Korea's economic discrimination more generally, the KFTC's targeted attacks on American-owned businesses have been going on for decades. In 2005, the KFTC fined Microsoft, America's third largest company at the time, $35.43 million for allegedly abusing its market dominance and issued "a corrective measure that is more stringent on Microsoft than that of the European Commission."[64] The KFTC forced Microsoft to sell an unbundled version of its operating system that did not include an instant messaging feature or Windows Media Player.[65] The then-Deputy Assistant Attorney General for the Antitrust Division criticized the decision, explaining that "Korea's remedy goes beyond what is necessary or appropriate to protect consumers, as it requires the removal of products that consumers may prefer."[66]

According to a 2007 report from the Information Technology and Innovation Foundation, a nonprofit research organization that specializes in technology policy, the KFTC's investigation followed a series of complaints by two of Microsoft's largest Korean competitors, Daum

---

[58] CPNG-HJC119-0000421; *see also* CPNG-HJC119-0001715.
[59] Abbott, *supra* note 27.
[60] CPNG-HJC119-0000421, at 422.
[61] *See* Jiyoung Sohn, *Google Fined $177 Million in South Korea Over Thwarting Potential Android Rivals*, WALL STREET JOURNAL (Sept. 14, 2021).
[62] CPNG-HJC119-0001706; Kim Bo-eun, *Korea Fines Google W207 Bil. for Abuse of Market Dominance*, KOREA TIMES (Sep. 14, 2021).
[63] *See* Bo-eun, *supra* note 62.
[64] Youngjin Jung & Seung Wha Chang, *Korea's Competition Law and Policies in Perspective*, 26 NW. J. INT'L L. & BUS. 687, 688 (2006); *South Korea to let Microsoft drop antitrust appeal*, REUTERS (Oct. 16, 2007); Gary Hoover, *Most Valuable American Companies over 30 Years: 1995-2025*, AM. BUS. HIST. CTR. (Jul. 17, 2025).
[65] *See* Press Release, U.S. Dep't of Justice, Statement of Deputy Assistant Attorney General J. Bruce McDonald Regarding Korean Fair Trade Commission's Decision in its Microsoft Case (Dec. 7, 2005).
[66] *Id.*

Communications and NateOn, that its instant messaging service was harming their businesses.[67] Even more, "[t]he KFTC later expanded its investigation to focus on Microsoft's Media Player, which competes with similar products made by Sanview and DideoNET, also Korean companies."[68] Notably, "[t]he KFTC's decision makes Microsoft's products less competitive versus its domestic competitors' applications . . . by forcing the company to assume the costs of the redesign" and "by forcing Microsoft to promote the software applications of these Korean companies."[69]

In 2025, the NBR conducted a series of interviews with representatives of American businesses that have been targeted by the KFTC.[70] Every company representative interviewed by the NBR "reported recurrent, burdensome, and unpredictable actions" designed to target American-owned companies and limit their ability to effectively compete against Korean companies.[71] The report's "findings indicate that the KFTC's enforcement practices are clearly protectionist when compared with those of other jurisdictions."[72]

1. Denial of Due Process and Procedural Fairness

The American business representatives interviewed by the NBR consistently emphasized a "[l]ack of due process and procedural fairness" in KFTC proceedings.[73] The KFTC intentionally withholds information from American businesses during investigations, preventing them from understanding what they are even being accused of and hindering their ability to defend themselves.[74] These businesses are routinely subjected to requests for information and company data that are exceedingly broad and overly burdensome.[75] Worse yet, the companies often "lack the opportunity to challenge or clarify information or allegations that the KFTC receives from other parties" and are denied the ability to "proffer a defense or rebut the evidence against them prior to the penalty being determined."[76] These problems are exacerbated by the fact that targets of the KFTC's discriminatory enforcement practices have virtually no ability to contest the evidence, rationale, or scope of an investigation in court before the KFTC issues a decision.[77] As a result, American companies are never given a meaningful opportunity to challenge the KFTC either before the agency itself or in a court of law prior to the agency making its final determination in an investigation.[78]

In addition, the KFTC often launches frivolous investigations into U.S. companies that are based "on single, anonymous complaints without clear, substantiated accusations of

---

[67] *See* Julie A. Hedlund & Robert D. Atkinson, *The Rise of the New Mercantilists: Unfair Trade Practices in the Innovation Economy*, ITIF (June 2007), at 13.
[68] *Id.*
[69] *Id.*
[70] *See* CPNG-HJC119-0000421, at 422.
[71] *Id.*
[72] *Id.*
[73] *Id.* at 423.
[74] *See id.*
[75] *See id.*
[76] *Id.* at 423-24.
[77] *See id.* at 424.
[78] *See id.* at 423-24.

wrongdoing."[79] American business leaders interviewed by the NBR report that antitrust investigations targeting their companies occur with unusual frequency and on a predictable cycle in a way that strongly suggests the KFTC is being pressured to maintain a steady cadence of enforcement actions against U.S. companies.[80] Rather than going after businesses for actual anticompetitive conduct, these investigations are often focused on "minor technical or business decisions that are clearly not anticompetitive, such as ceasing orders or relationships that are unprofitable."[81] Notably, companies report that "the KFTC appears responsive to complaints from Korean firms," especially in situations where an American company has recently entered a market that is currently dominated by Korean companies.[82]

2. Aggressive Investigative Tactics

According to the NBR, KFTC investigations are "characterized by unnecessarily aggressive tactics, including the *pro forma* use of unannounced dawn raids at the start of an investigation," with the "prevailing experience" being "one of hostility and pressure to comply."[83] In fact, the KFTC regularly uses Korea's broad charge of obstruction "to coerce or intimidate employees into compliance."[84] As NBR explains:

> During dawn raids and subsequent investigations, staff are subjected to intense, prolonged interviews, often at both company offices and KFTC premises. They are frequently required to sign KFTC prepared statements before being allowed to leave. Staff recount cases where investigators scream at their legal counsel and demand access to employee devices, even when this is physically impossible because passwords from staff who are not present are unavailable. The psychological toll can be significant. The situation is made more challenging because the KFTC often threatens individual employees with criminal obstruction of justice charges if they do not comply with KFTC requests, even when the requests are overly broad or not relevant to the investigation, forcing them to sign statements confirming that they are personally refusing a KFTC request and that they are aware that this may amount to obstruction.[85]

Similarly, the NBR found that the KFTC regularly abuses its "broad (and largely unconstrained) authority to request and seize huge amounts of information during raids and investigations."[86] American companies operating in South Korea "face repeated, broad, and onerous requests for data and information from the KFTC, including demands for highly

[79] *Id.* at 424.
[80] *See id.* at 425.
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.* at 426.
[85] *Id.*
[86] *Id.*

sensitive proprietary data such as source code."[87] These requests create massive administrative burdens for regulated companies and "expose them to risks of competitive harm, reputational damage, and the loss of intellectual property."[88] This is exacerbated by the fact that South Korea does not provide companies with the same ability to challenge regulatory agencies' information requests in court that they receive in the United States and other developed countries, nor does it recognize attorney-client privilege.[89]

Perhaps most concerning, the KFTC has increasingly used criminal charges to punish American companies for commonplace regulatory violations, a practice that is exceedingly rare among other antitrust enforcement agencies across the globe.[90] American companies have described this "as a key tool in [the KFTC's] efforts to intimidate firms and their employees to provide whatever information it wants and to not push back against overreach."[91] While most countries only allow for the criminal enforcement of competition laws in extremely limited circumstances, the KFTC has the broad power to issue criminal referrals for almost any regulatory violation.[92] Rather than exercising this power with caution, the KFTC has actually increased its use of criminal referrals significantly in recent years.[93] In March 2021, the KFTC fined Apple, an American company, ₩300 million (approximately $264 thousand) and sought criminal charges against one of its executives.[94]

Notably, "[t]he KFTC's actions do not occur in isolation," but instead "reflect a broader South Korean policy perspective that views competition policy primarily as a domestic tool, with limited regard for international trade obligations."[95] South Korea has shown a persistent willingness to use any tools at its disposal to disadvantage American companies and insulate South Korean companies from competition, including the creation of new laws, regulations, and enforcement authorities.

C. South Korea Uses Digital Laws and Regulations to Harm American Companies

South Korea's anticompetitive approach to economic regulation can be seen in its development of digital laws and regulations specifically designed to harm American-owned businesses, such as its ongoing consideration of platform regulations based on the European Union's discriminatory Digital Markets Act (DMA). In December 2023, the KFTC released a legislative proposal modeled directly on the DMA, the Platform Competition Promotion Act (PCPA).[96] The PCPA would subject digital platforms operating in South Korea to a set of prohibitive and overly burdensome regulatory obligations like those contained in the DMA.[97]

---

[87] *Id.*
[88] *Id.* at 427.
[89] *See id.* at 426.
[90] *See id.* at 428.
[91] *Id.*
[92] *See id.* at 428.
[93] *See* Lee, *supra* note 36.
[94] *See* Julie Masson, *Apple Faces Criminal Charges for Obstructing Probe in Korea*, GLOBAL COMPETITION REVIEW (Mar. 31, 2021).
[95] CPNG-HJC119-0000421.
[96] *See* Kiss, *Will Korea Burn Its Digital Future Down?*, *supra* note 12.
[97] *See id.*

The KFTC would enforce these regulations by "[p]re-designating a select number of core platforms as 'dominant platform operators' that possess the power to control the platform market" and prohibiting these platforms from engaging in certain "abusive practices."[98]

The KFTC's decision to advance DMA-style legislation reflects the discriminatory nature of its regulatory regime. The European Union specifically designed the DMA to target American companies and hinder their ability to effectively compete in foreign markets.[99] European policymakers repeatedly reaffirmed the fact that the goal of the DMA was to address Europe's economic stagnation by adopting burdensome regulations and using aggressive enforcement tactics against U.S. companies to strengthen the position of their European competitors.[100] By its very design, six of the seven businesses targeted by the DMA are American companies or wholly owned subsidiaries of American companies.[101] Like the DMA, the PCPA is an anticompetitive attempt to weaponize competition law in order to hinder the ability of American companies to compete in the global economy.

Under the PCPA, the KFTC would be empowered to "target specific firms" and "establish thresholds to designate dominant firms and platforms (so-called gatekeepers) that align with the claimed market power of large U.S. tech firms."[102] According to the NBR, it is "clear that U.S. firms are the ones South Korea seeks to target" as "the KFTC exempts smaller firms and, in effect, Chinese rivals."[103] American businesses have explicitly warned that the regulatory requirements contained in the PCPA would "trample on competition that clearly benefits consumers, ignore good regulatory practices fundamental to sound regulatory models, and place governments in a position of violating their trade commitments by arbitrarily targeting foreign firms."[104]

After receiving considerable pushback from U.S. businesses and antitrust experts, the KFTC released an alternative proposal known as the Partial Amendment Bill (PAB).[105] The PAB would amend South Korea's existing antitrust law in order to prevent so-called "dominant online platform operators" from engaging in normal business practices like drawing attention to their own offerings and combining various products and services together for consumers.[106] While

---

[98] Kyung-Hwan Chung & Hye Sook Seo, *South Korea: Fresh online platform regulations kickstart new era of antitrust law*, GLOBAL COMPETITION REVIEW (Nov. 27, 2024).
[99] *See* Espinoza, *supra* note 13; Charanzová, *supra* note 13; *Europe is now a corporate also-ran. Can it recover its footing?*, *supra* note 13; Draghi, *The Future of European Competitiveness Part B | In-depth analysis and recommendations*, EUROPEAN COMMISSION 302 (Sept. 2024); Federico Steinberg & Max Bergmann, *The Draghi Report: A Strategy to Reform the European Economic Model*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (Oct. 2, 2024).
[100] *See* Espinoza, *supra* note 13; Charanzová, *supra* note 13; *Europe is now a corporate also-ran. Can it recover its footing?*, *supra* note 13; Draghi, *supra* note 99; Steinberg & Bergmann, *supra* note 99.
[101] *See* European Commission, *Gatekeepers* (last visited Jul. 7, 2025).
[102] CPNG-HJC119-0001715.
[103] *Id.*
[104] Freeman, *supra* note 12.
[105] *See id.*; Jin Yu Young & Daisuke Wakabayashi, *The Antitrust Enforcers Aimed at Big Tech. Then Came the Backlash*, N.Y. TIMES (Feb. 16, 2024); Andrew Yeo, *South Korea's Digital Regulation Proposal Sparks U.S. Pushback*, LAWFARE (May 20, 2025);
[106] CPNG-HJC119-0001715; Lilla Nóra Kiss, *Why South Korea Should Resist New Digital Platform Laws*, *supra* note 12.

South Korea has presented the PAB as a less aggressive approach to platform regulation, experts have noted that it "effectively replicates DMA-style provisions—such as structural presumptions and expanded theories of harm—into traditional antitrust law" and poses the same risk of "regulatory overreach without clear justification."[107] On July 24, 2025, the Committee and Subcommittee sent a letter to KFTC Chairman Han Ki-jeong raising these concerns and the potential effect that discriminatory platform regulations could have American businesses.[108] Despite repeated warnings from United States officials,[109] South Korea has continued to advance anticompetitive digital platform regulations intentionally designed to harm American businesses.[110]

This is not the first time that South Korea has created new digital regulations with the explicit goal of punishing innovative American companies. On August 31, 2021, just days before the KFTC fined Google approximately $176.6 million, the South Korean parliament enacted a bill to amend the Telecommunications Business Act, often referred to as the "Anti-Google law."[111] The amendments included in this bill prohibit Google and Apple from controlling the payments systems used by developers seeking access to their app stores.[112] While these types of prohibitions hinder innovation, promote fraud, and create major privacy and security risks for consumers, they directly benefit large Korean developers who want access to American-owned app stores without having to comply with their contractual requirements.[113]

Outside of digital platforms, the Korea Internet & Security Agency (KISA)'s Cloud Security Assurance Program (CSAP) has been used to impose undue burdens on U.S. cloud service providers.[114] CSAP is a collection of regulatory requirements created in 2016 that cloud service providers must comply with in order to work with South Korea's public institutions.[115] Among other obligations, CSAP requires cloud operations, backup systems, management personnel, and data to all be physically located in South Korea.[116] In addition, "CSAP mandates the use of Korea-specific encryption standards and discourages logical (software-based) network separation for moderate-tier workloads, instead favoring physical separation even when it is not technically necessary."[117] These requirements "effectively limit foreign cloud service providers' access to the public sector cloud market" and act "as protectionist measures favoring domestic

---

[107] Robert D. Atkinson & Sejin Kim, *South Korean Policy in the Trump and China Era: Broad-Based Technological Innovation, Not Just Export-Led Growth*, ITIF (May 18, 2025).
[108] *See* July 24 Letter, *supra* note 12.
[109] *See* CPNG-HJC119-0000001, at 260-61; CPNG-HJC119-0000405; Robert C. O'Brien, *South Korea's proposed tech regulations would be a gift to China*, THE HILL (Dec. 28, 2023); Kim Eun-jin, *South Korea's Platform Law Faces Criticism, Potential Trade Clash with U.S.*, BUSINESS KOREA (Feb. 18, 2025); Gavin Bade & Amrith Ramkumar, *U.S. Warns Korea Against Targeting American Tech Firms Amid Trade Escalation*, WALL STREET JOURNAL (Jan. 27, 2026).
[110] *See* Nigel Cory, *South Korea's Online Platform Fairness Bill: A New Digital Nontariff Barrier in U.S.-ROK Trade*, NATIONAL BUREAU OF ASIAN RESEARCH (Feb. 25, 2026).
[111] Ella Geris, *South Korea passes 'anti-Google law'*, JURIST (Sept. 2, 2021).
[112] *See id.*
[113] *See generally* Joseph V. Coniglio & Matthew Kilcoyne, *Comments to UK CMA Regarding Recent Developments in Relation to Apple's and Google's App Store Rules*, ITIF (Apr. 24, 2026).
[114] *See South Korea's Cloud Service Restrictions*, *supra* note 14; CCIA, *supra* note 14, at 168.
[115] *See* CPNG-HJC119-0000001, at 259; *South Korea's Cloud Service Restrictions*, *supra* note 14; CCIA, *supra* note 14, at 168.
[116] *See South Korea's Cloud Service Restrictions*, *supra* note 14; CCIA, *supra* note 14, at 168.
[117] *South Korea's Cloud Service Restrictions*, *supra* note 14; CCIA, *supra* note 14, at 168.

companies."[118] On March 3, 2026, eleven Members of Congress sent a letter to United States Trade Representative Jamieson Greer raising concerns about South Korea's CSAP discriminatory requirements and encouraging the Trump Administration to address these issues in U.S.-Korea trade negotiations.[119]

II. SOUTH KOREA HAS WEAPONIZED ITS GOVERNMENT AGENCIES TO ATTACK COUPANG

One recent and glaring example of South Korea's protectionist abuse of government power is its discriminatory treatment of Coupang, an American-owned e-commerce company whose rapid growth and competitive success have made it a consistent target of the South Korean government.[120] South Korea has repeatedly subjected Coupang to overly aggressive enforcement practices and unfair treatment in an effort to protect its Korean competitors.[121] This discrimination has included the initiation of ceaseless investigations and onsite inspections, punitive regulatory obligations, retaliatory enforcement decisions, excessive fines, and even criminal charges against American citizens.[122] South Korea's unwarranted attacks on Coupang violate fundamental principles of due process and hinder the company's ability to meaningfully participate in the global economy.

A. South Korea Has Repeatedly Targeted Coupang for Hostile Regulatory Treatment

South Korea has engaged in a multi-year harassment campaign specifically designed to attack Coupang and prevent the American-owned company from effectively competing in the South Korean market. Coupang is an innovative e-commerce company headquartered in Seattle, Washington, and incorporated in Delaware that operates retail, food delivery, and video streaming services across Asia.[123] It is commonly described as "the Amazon of South Korea" and has invested billions of dollars in the South Korean market.[124] Coupang is currently the second-largest private employer in South Korea, operating over 100 different fulfillment centers and distributing more than $5 billion in American goods and services in 2025 alone.[125]

However, far from embracing Coupang and the innovative services it provides to Koreans, South Korea has done everything in its power to force the American retailer out of the Korean market. In deposition testimony, Coupang's interim CEO Harold L. Rogers documented South Korea's long history of discriminatory treatment against Coupang.[126] According to Mr.

---

[118] *South Korea's Cloud Service Restrictions*, *supra* note 14; Kim Eun-joong, *U.S. Lawmakers Demand South Korea Drop Cloud Barriers*, CHOSUN DAILY (Mar. 6, 2026); *see also* Letter from Rep. Carol Miller et al. to Hon. Jamieson Greer, United States Trade Representative (Mar. 3, 2026).
[119] *See* Letter from Rep. Carol Miller et al. to Hon. Jamieson Greer, United States Trade Representative (Mar. 3, 2026).
[120] *See* CPNG-HJC119-0000421; Yonhap, *supra* note 15; *Spy agency requests Natl Assembly to charge Coupang chief over alleged perjury*, *supra* note 15; Yonhap, *supra* note 15.
[121] *See* CPNG-HJC119-0000421; Yonhap, *supra* note 15; Deposition of Mr. Harold L. Rogers, *supra* note 15.
[122] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15; CPNG-HJC119-0000421.
[123] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 9.
[124] Gina Heeb, *Coupang—The Amazon Of South Korea—Just Became The Largest Foreign IPO On Wall Street Since Alibaba. Here's What You Need To Know*, FORBES (Mar. 11, 2021); Deposition of Mr. Harold L. Rogers, *supra* note 15, at 11.
[125] *See Economic Impact*, COUPANG (last visited May 8, 2026); *About Us*, COUPANG (last visited May 8, 2026).
[126] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15.

Rogers, South Korea is continually "working to drive customers away from [Coupang] and drive them to . . . a Korean competitor."[127] He described South Korea as "the most difficult regulatory environment" he has ever worked in, and Coupang's relationship with South Korean regulators as "antagonistic" and, in many cases, "retaliatory."[128]

Like other American companies, Coupang has been subjected to abusive enforcement practices and egregious due process violations by the South Korean government. South Korean regulators regularly conduct "dawn raids," in which they "show up unannounced in [Coupang's] lobby in the morning and demand immediate access to [Coupang's] offices."[129] Coupang was subjected to over 400 inspections by the Ministry of Employment and Labor alone in 2025.[130] According to Mr. Rogers, "[i]f you walk into [Coupang's] main office building in Seoul . . . 1 in 10 people that you run into . . . is a Korean investigator."[131] Coupang is forced to devote approximately 100 different employees to complying with demands from Korean regulatory agencies.[132] Additionally, Mr. Rogers testified that in order to comply with Korea's laws and regulation, Coupang hires "basically every large Korean law firm" as well as "multiple U.S. law firms."[133]

During these raids, Mr. Rogers recounted, investigators "roam [Coupang's] halls . . . and grab employees to interrogate them," taking their "documents," "computers," and "personal devices, and seiz[ing] them."[134] Investigators will often "[p]ut people in conference rooms for hours on end, often until 2, 3, 4 a.m. in the morning, questioning them, generally without allowing [employees] to have counsel present with them."[135] Even though investigators often exceed their authority during these raids, they "still demand [Coupang's] compliance and threaten [Coupang] with sanctions, turning a civil investigation into a criminal investigation, or opening new multiple investigations if [Coupang] [doesn't] comply with their requests."[136] During their interrogations, investigators will scream at employees, "insulting" and "berating" them.[137]

Mr. Rogers explained that similar to other American-owned businesses operating in South Korea, "[t]he amount of data that [Coupang] [is] often being asked for and the timelines that are given" make it "physically impossible" for the company to comply.[138] He testified that these requests often require the production of "thousands and thousands of documents" as well as terabytes of data that would take "days to be able to just download."[139] In spite of this, South Korean regulators demand that these materials are "produced to them by end of day."[140] Mr.

---

[127] *Id.* at 109.
[128] *Id.* at 15-16.
[129] *Id.* at 13.
[130] *See id.* at 22, 111.
[131] *Id.* at 13.
[132] *See id.* at 74.
[133] *Id.* at 74.
[134] *Id.* at 13.
[135] *Id.* at 13, 24.
[136] *Id.* at 13-14.
[137] *Id.* at 24-26.
[138] *Id.* at 72.
[139] *Id.*
[140] *Id.*

Rogers testified that these "physically impossible" demands "always come[] with the threat of criminal action if [Coupang] [doesn't] comply."[141] Notably, South Korean regulators regularly use the threat of making additional document requests, initiating new investigations, and even escalating civil fines into criminal charges to extract concessions from American companies.[142] The KFTC, the Korea Media and Communications Commission, the Ministry of Employment and Labor, and members of the National Assembly have each threatened to suspend Coupang's business operations.[143]

Mr. Rogers explained that South Korean regulators "routinely demand documents that are in the United States," and when Coupang raises "jurisdiction or venue questions," they are "once again . . . threatened with immediate criminal action if [Coupang] [doesn't] turn them over immediately."[144] According to Mr. Rogers, Korean regulators insist on these demands even when doing so may impact Coupang's ability to comply with United States laws and regulations.[145]

The Korean production demands are not limited to information regarding the specific conduct being investigated by a given agency.[146] Mr. Rogers testified that Korean officials use a "regular tactic" where "one regulatory authority [will] come in and make incredibly broad requests that are oftentimes irrelevant to the conduct they're actually investigating . . . [a]nd then they'll provide those to another regulator that'll use them to initiate an investigation against [Coupang]."[147] Even more concerning, the information that Coupang provides to South Korean regulators, including trade secrets and confidential documents, is sometimes leaked to its Korean competitors.[148]

Mr. Rogers testified that South Korean officials favor Coupang's competitors specifically "because they are Korean companies."[149] According to him, government officials are "driving [consumers] to Korean companies and Chinese companies that are in lucrative joint ventures with Korean companies."[150] In fact, the few "American companies [that] have been allowed to compete in Korea," were able to do so primarily by "enter[ing] into a lucrative joint venture with a large Korean company."[151] Others enter into joint ventures with the Korean government itself in "an effort . . . to try and get the Korean government to treat [the company] fairly."[152]

Like many other American companies, the KFTC is Coupang's primary and most aggressive regulator in South Korea.[153] According to a report that the KFTC submitted to the National Assembly, between 2022 and the first half of 2025, the agency fined Coupang a total of

---

[141] *Id.*
[142] *See id.* at 13-14, 77.
[143] *See id.* at 77; CPNG-HJC119-0001709.
[144] *Id.* at 72.
[145] *See id.* at 73.
[146] *See id.*
[147] *Id.*
[148] *See id.* at 26-27.
[149] *Id.* at 109.
[150] *Id.*
[151] *Id.* at 110-11.
[152] *Id.*
[153] *Id.* at 12.

₩162.8 billion (approximately $114.3 million).[154] This amount was the largest collection of fines imposed by the KFTC on any single company during the period and exceeded the next highest amount by over ₩40 billion, even though Hyundai, Hanssem, SK Group, and several other Korean companies had far more comparable legal violations than Coupang during that same period.[155]

The KFTC has even criticized Coupang for charging prices that it considered to be too low and pushed the company to increase its prices, which Mr. Rogers commented is "the exact opposite of what you would expect to see from a competition authority that would want that kind of competition and would want generally lower prices for consumers."[156]According to Mr. Rogers, Coupang is "not getting scrutiny for [its] practices," it is "getting scrutiny for the fact that [its] an American company" that is "beating Korean companies in their markets, which is something they do not want." [157]

B. South Korea Has Escalated its Attacks on Coupang and Threatened American Citizens with Criminal Charges, Using Corporate Espionage as a Pretext for Intrusive Investigations

The ongoing response by the South Korean government to a recent incident in which a disgruntled former employee accessed Coupang's data systems without authorization serves as a particularly egregious example of its discriminatory attacks on American-owned companies. This can be seen as a case study of how South Korea weaponizes its government agencies to attack foreign companies and, particularly, American businesses. After a disgruntled former Coupang employee used a stolen key to download a limited amount of customer data from Coupang, the South Korean government launched a massive, "whole-of-government assault on Coupang," spreading false information about the scope of the unauthorized access and initiating dozens of frivolous and, in many cases, unrelated investigations into Coupang's business practices.[158] While these investigations were still ongoing, South Korean officials continually attacked Coupang in the media, referring to the company as a criminal organization and threatening to suspend its business operations.[159]

According to Mr. Rogers, before any investigation actually took place, "leaders in the country, like the President and Prime Minister, prejudged what had occurred, said that it was the worst leak in the history of Korea," and said that Coupang "needed to be put out of business."[160] Even more, after Coupang engaged in an extensive operation to recover the devices that the former employee used to store the stolen customer data at the explicit direction of South Korea's National Intelligence Service (NIS), the South Korean government denied its involvement in the

---

[154] *See* Yonhap, *Coupang tops FTC fine among Korean conglomerates over past 3 yrs: report*, KOREA HERALD (Oct. 19, 2025).
[155] *See* Kim Jisun, *Coupang Tops List of Companies Fined Most by Korea Fair Trade Commission Over the Past 3.5 Years*, ALPHABIZ (Oct. 20, 2025).
[156] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 79-82.
[157] *Id.* at 123.
[158] CPNG-HJC119-0001673, at 1675; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 77;
[159] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 77, 128-40; CPNG-HJC119-0000455; CPNG-HJC119-0000631; CPNG-HJC119-0001597, at 1604-07; CPNG-HJC119-0001709.
[160] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 83.

operation and filed criminal complaints against Mr. Rogers, an American citizen, and several other Coupang executives.[161] Coupang has been targeted by South Korea and subjected to discriminatory treatment for years, but following the unauthorized access, as Coupang investors recently explained in a petition to the USTR, "the Korean Government's hostility has escalated into a coordinated effort to cripple Coupang's operations."[162] On June 11, 2026, South Korea fined Coupang over $410 million for the incident, the largest fine ever imposed on a single company, which far exceeds fines imposed on South Korean companies for data breaches that were far more serious and involved highly sensitive personal information.[163]

1. The Former Employee's Unauthorized Access of Coupang's Data Systems

According to documents produced to the Committee and Subcommittee, on November 18, 2025, Coupang's information security team confirmed that a disgruntled former employee had stolen an "alphanumeric fallback key,"[164] a specific type of digital password, and used it to access certain categories of "low-sensitivity data" related to specific customer accounts, such as names, emails, and phone numbers.[165] The former employee was a Chinese national who worked as a senior engineer for Coupang designing backup login mechanisms and stole the key after the company terminated his employment.[166] Following his termination, the employee returned to China and used the stolen key to access Coupang's internal system, search for customer information, and download a limited subset of that information onto local devices.[167] While the key provided access to information associated with as many as 33.7 million accounts, the former employee only stored and retained information related to approximately 3,000 accounts.[168]

Coupang disclosed the unauthorized access to the Korea Internet & Security Agency (KISA) the following day, November 19, and the Personal Information Protection Commission (PIPC) on November 20.[169] On November 29, Coupang issued a press release to inform the public of the incident and confirm the number of customer accounts affected by the breach.[170] On November 30, the then-CEO of Coupang Corp., Park Dae-jun, attended a meeting with several high-ranking members of the South Korean government, including the Deputy Prime Minister Bae Kyung-hoon, acting Commissioner General of the National Police Agency Yoo Jae-sung, and the Third Deputy Director of the National Intelligence Service (NIS) Kim Chang-seop.[171] During this meeting, Mr. Park issued a formal apology for the incident, answered

[161] *See infra* Sections II.B.1, II.B.2.
[162] CPNG-HJC119-0001673, at 1676.
[163] Jun, *supra* note 26; Gyu-lee, *supra* note 26.
[164] An alphanumeric fallback key is a digital password containing a combination of letters, numbers, and symbols.
[165] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 66, 83, 87. This employee did not access any high-sensitivity data, such as financial information, medical records, or login credentials. *Id.* at 88; CPNG-HJC119-0000833; CPNG-HJC119-0001596.
[166] *See* CPNG-HJC119-0000836, at 845; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 83.
[167] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 88-89.
[168] *See id.* at 88. The scope of this incident was subsequently confirmed by leading cybersecurity companies including Mandiant and Palo Alto Networks as well as by sworn statements from the former employee. *Id.* at 89.
[169] *See* CPNG-HJC119-0001549, at 1562; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 87.
[170] *See Coupang here to inform you*, COUPANG (Nov. 29, 2025).
[171] *See* CPNG-HJC119-0001070, at 1076; CPNG-HJC119-0000887, at 926; CPNG-HJC119-0001549, at 1564; CPNG-HJC119-0002057; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 91; Ko Dong-hwan, *Coupang apologizes over info leak affecting 33.7 mil. Customers*, KOREA TIMES (Nov. 30, 2025).

questions from government officials, and addressed the need to recover any devices that the disgruntled former employee had used to store customer data.[172]

Around 2:00 p.m. the next day, December 1, 2025, NIS contacted Coupang for the first time and requested a meeting for later that day at the company's corporate office in Seoul.[173] At approximately 4:00 p.m. that afternoon, two Director-level officials from NIS arrived at the company's corporate office and asked a representative from Coupang (referred to in the documents and hereinafter as "Arthur") to keep the contents of the meeting "confidential, whether internally or externally."[174] Arthur would serve as Coupang's primary point of contact with NIS going forward.[175] According to documents produced to the Committee and Subcommittee, the officials told Arthur that the "meeting was an extension" of the one that Mr. Park attended the day before and "immediately positioned the situation as a cooperative effort" to recover the devices that the former employee used to retain customer information.[176] The officials indicated that "NIS was very interested in getting these devices back and working with Coupang in order to retrieve them."[177] NIS "need[ed] [Coupang's] significant cooperation" as the devices were still in the disgruntled former employee's possession at the time and "NIS couldn't operate in China."[178] The NIS officials "told [Coupang] that they were part of the joint government investigation," and that Coupang was "legally required" to "work with them."[179]

Later that evening, Arthur contacted the Director of the NIS Investigations Division and asked whether Coupang "ha[d] an obligation to follow these requests."[180] After the Director confirmed that "Coupang had a legal obligation to cooperate" with NIS,[181] Arthur asked the Director to have NIS "send [Coupang] an explicit written document describing the grounds" for this legal obligation in the form of "an official letter."[182] The Director agreed, and less than twenty-four hours later, on December 2, 2025, NIS sent Coupang "an official letter [that] explicitly cited Article 5 of the National Intelligence Service Korea Act" and confirmed that Coupang "had a legal obligation to comply with the NIS's request."[183]

---

[172] *See* CPNG-HJC119-0001070, at 1076; CPNG-HJC119-0000887, at 926; CPNG-HJC119-0002057; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 91; Dong-hwan, *supra* note 171.
[173] *See* CPNG-HJC119-0000887, at 929-32; CPNG-HJC119-0001070, at 1077; CPNG-HJC119-0001549, at 1564; CPNG-HJC119-0002056; CPNG-HJC119-0002057, at 2058; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 92.
[174] CPNG-HJC119-0000887, at 937; CPNG-HJC119-0002057, at 2058.
[175] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 90; CPNG-HJC119-0000887.
[176] CPNG-HJC119-0000887, at 937-38; CPNG-HJC119-0001070, at 1077; CPNG-HJC119-0001549, at 1565; CPNG-HJC119-0002057, at 2058.
[177] CPNG-HJC119-0000887, at 944; CPNG-HJC119-0001549, at 1565; CPNG-HJC119-0002057, at 2058; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 92.
[178] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 92-93; CPNG-HJC119-0000887, at 944-45; CPNG-HJC119-0001549, at 1565; CPNG-HJC119-0002057, at 2058.
[179] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93; *see also* CPNG-HJC119-0002057, at 2058.
[180] CPNG-HJC119-0000887, at 945; *see also* CPNG-HJC119-0002056; CPNG-HJC119-0002057, at 2058.
[181] CPNG-HJC119-0001070, at 1077; CPNG-HJC119-0002057, at 2058; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93.
[182] CPNG-HJC119-0000887, at 945; CPNG-HJC119-0001070, at 1077; CPNG-HJC119-0002057, at 2058.
[183] CPNG-HJC119-0001070, at 1077-78; CPNG-HJC119-0001549, at 1565-66; CPNG-HJC119-0002057, at 2058-59; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93-95.

I, [redacted] certify that I am competent to translate from Korean into English and that the translation of the below document is true, accurate, and complete to the best of my knowledge. This translation has been reviewed and verified by a human translator. If you have any questions regarding the translation, please contact me at the email address below.

Typed Name: [redacted]
Qualifications: Professional Translator with an MA in Korean-English Interpretation, Seoul, Korea
Email: [redacted]@coupang.com
Date: February 4, 2026

[Translation of the official letter from the NIS]

National Intelligence Service (Republic of Korea)

Recipient: Representative Director of Coupang Corp. (via appropriate internal channels)

Subject: Request for Cooperation in Operational Matters Necessary for the Verification and Investigation of Cybersecurity Threats

1. **Relevant Legal Basis**

   a. Article 4, Paragraph 1, Subparagraph 1(b) of the National Intelligence Service Korea Act: Collection, preparation, and distribution of intelligence on counterespionage, counterterrorism, and international criminal syndicates.
   b. Article 4, Paragraph 1, Subparagraph 1(e) of the National Intelligence Service Korea Act: Collection, preparation, and distribution of intelligence on cybersecurity, including international and national hacker organizations.
   c. Article 4, Paragraph 1, Subparagraph 3 of the National Intelligence Service Korea Act: Measures to identify, monitor, deter, and block activities threatening national security, and to protect the safety of the public.
   d. Article 5, Paragraphs 1 and 2 of the National Intelligence Service Korea Act: Requests for submission of materials and cooperation from state agencies and other entities, and conduct of investigations.
   e. Articles 102 and 103 of the Basic Guidelines for National Crisis Management: Establishment and operation of the National Cyber Crisis Management Group for a coordinated government response.

2. The National Intelligence Service (including the National Cyber Crisis Management Group), as part of a coordinated government response, request the submission of relevant materials for cause analysis and response measures. We ask for your cooperation in this matter. End of Document.

Translation of the official letter confirming Coupang's legal obligation to comply with NIS's directions.[184]

[184] CPNG-HJC119-0000880, at 882.

Coupang subsequently hired two of the largest law firms in South Korea to independently review the NIS demand letter, both of which concluded "that, under Korean statutes, [Coupang] w[as] required to comply with the NIS" and its requests.[185] While NIS's letter is framed as a "request for cooperation," both law firms advised Coupang that "pursuant to the statutory requirements of Article 5 of [South Korea's] National Intelligence Service Act," the company "was under an obligation to comply with the National Intelligence Service's request for cooperation."[186] Even though the letter was "styled as a 'request,' a National Intelligence Service[] demand for cooperation is not optional as a matter of Korean law."[187] Additionally, according to deposition testimony, NIS continually affirmed to Coupang that the request was mandatory, explaining that "the company must comply" with NIS's requests.[188] In other words, NIS's requests were not voluntary—as lawyers advised and NIS itself affirmed, the requests created formal obligations that Coupang was legally required to follow.[189]

2. The NIS-Directed Recovery Operation

Documents produced to the Committee and Subcommittee suggest that the evening of December 2, 2025, Arthur had a face-to-face meeting with NIS officials and told them that Coupang would cooperate with their investigation.[190] The officials "said that all future cooperation and communication would be conducted solely via phone calls and face-to-face meetings" and "emphasized the need for strict confidentiality."[191] During this meeting, "talks about the retrieval of materials came out in earnest" and "the attendees unanimously agreed that a swift recovery, above all else, is the best approach to prevent the situation from escalating into a security or diplomatic issue and to alleviate public anxiety."[192]

Based on NIS's request for strict confidentiality, Coupang sought guidance from NIS on whether it should inform South Korea's national police about this recovery operation.[193] NIS said that "they would be coordinating with the police and would take care of" any communication that needed to occur, and that Coupang "didn't need to worry about that."[194] When Coupang continued to express concern about withholding information from the police,

---

[185] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93-95; *see also* CPNG-HJC119-0001509, at 1528-29; CPNG-HJC119-0001549, at 1566; CPNG-HJC119-0001597, at 1616-17; CPNG-HJC119-0002057, at 2057-59.
[186] CPNG-HJC119-0001995, at 2004-05; *see also* CPNG-HJC119-0002057, at 2057-59.
[187] CPNG-HJC119-0002057, at 2057-59.
[188] CPNG-HJC119-0000887, at 966; CPNG-HJC119-0002057, at 2057; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93-95.
[189] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93-95; *see also* CPNG-HJC119-0000887, at 966; CPNG-HJC119-0001509, at 1528-29; CPNG-HJC119-0001549, at 1566; CPNG-HJC119-0001597, at 1616-17; CPNG-HJC119-0001995, at 2004-05; CPNG-HJC119-0002057, at 2057.
[190] *See* CPNG-HJC119-0001070, at 1079; CPNG-HJC119-0000887, at 960-64; CPNG-HJC119-0001549, at 1567; CPNG-HJC119-0002057, at 2058-59.
[191] CPNG-HJC119-0001070, at 1079; CPNG-HJC119-0000887, at 960-64; CPNG-HJC119-0001549, at 1567-68; CPNG-HJC119-0002057, at 2059.
[192] CPNG-HJC119-0001070, at 1079; CPNG-HJC119-0000887, at 960-62; CPNG-HJC119-0001549, at 1567-68.
[193] *See* CPNG-HJC119-0000887, at 964; CPNG-HJC119-0001549, at 1568; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93.
[194] CPNG-HJC119-0000887, at 964; CPNG-HJC119-0001549, at 1568; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93.

NIS responded, "Didn't we . . . send an official document to Coupang? Since there is the [National Intelligence Service Korea] Act, the company must comply with it."[195]

On December 5, 2025, Coupang met with the NIS to discuss the technical aspects of the data breach.[196] During this meeting, NIS "became aware that the amount of personal information the suspect actually leaked might not be as much as known previously."[197] Mr. Rogers testified to the Committee and Subcommittee that despite becoming aware that the leak was limited in nature, NIS did not take any steps to correct the misconceptions that South Korean officials had spread about the scope of the leak, "nor did the [Joint Investigations Team], PIPC, KISA, or members of the National Assembly, who continued to let people believe that it was far larger and far more dangerous than it actually was."[198]

According to documents produced to the Committee and Subcommittee, on December 6, 2025, the former employee who had accessed Coupang's data systems without authorization sent a message to a group chat that included Coupang employees asking for the phone number of the company's legal department in Korea.[199] As soon as Coupang received this information, Arthur reported it to NIS.[200] In response, NIS instructed Coupang "to contact the [former employee] directly, even suggesting specific content and tone for the email" as well as "different ways to approach the [former employee] in order to get his cooperation."[201] Once again, NIS specifically directed Coupang not to share this information with the national police or any other government agencies.[202] At this time, NIS had repeatedly told Coupang that it would be "coordinating with the government officials" and "that [NIS officials] were . . . keeping the Presidential Office informed as to what was happening."[203]

According to contemporaneous notes, on December 8, 2025, NIS advised Arthur that it would be "natural for Coupang's legal team to make the initial contact with the" former employee and that if a "third-party" contacted the employee, he might suspect that it is the Korean police.[204] NIS told Arthur that the former employee "is currently residing at his address" in China, and that "[i]t does not appear that he is going to work or actively looking for a new job."[205] The following day, December 9, 2025, NIS suggested to Coupang specific cybersecurity firms in South Korea that the company should hire to analyze any data that might be recovered

---

[195] CPNG-HJC119-0000887, at 966.
[196] *See* CPNG-HJC119-0001070, at 1080; CPNG-HJC119-0001549, at 1569; CPNG-HJC119-0002057, at 2059; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 96.
[197] CPNG-HJC119-0001070, at 1080; CPNG-HJC119-0002057, at 2059; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 96-97.
[198] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 97.
[199] *See* CPNG-HJC119-0000887, at 983; CPNG-HJC119-0001070, at 1080; CPNG-HJC119-0001549, at 1568; CPNG-HJC119-0002056; CPNG-HJC119-0002057, at 2059.
[200] *See* CPNG-HJC119-0000887, at 983; CPNG-HJC119-0001070, at 1080; CPNG-HJC119-0001549, at 1568; CPNG-HJC119-0002056; CPNG-HJC119-0002057, at 2059.
[201] CPNG-HJC119-0001070, at 1080; CPNG-HJC119-0002056; CPNG-HJC119-0002057, at 2059; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 97.
[202] *See* CPNG-HJC119-0001070, at 1080; CPNG-HJC119-0002057, at 2059; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 97-98.
[203] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 98; *see also* CPNG-HJC119-0002056.
[204] CPNG-HJC119-0002056.
[205] *Id.*

from the former employee and said that "Korean companies would be better than American companies," as "[c]ompanies based in the U.S. are uncooperative with Korean investigative agencies."[206] In his notes from that day, Arthur specifically documented that "NIS is considering various approaches" to recovering the data, and that it was "clear that this is an NIS operation."[207]

Documents produced to the Committee and Subcommittee suggest that based on the NIS's directions, Coupang's legal team sent the former employee a message on December 9 requesting a meeting to discuss "technical matters" related to his unauthorized access of Coupang's system.[208] Because "they were getting worried that the former employee wasn't responding," the next day, NIS instructed Coupang to send another message to the suspect that included a response deadline.[209] Like with the previous communications, NIS instructed Coupang not to inform the police or other government agencies.[210] During these conversations, NIS suggested that it could not contact the former employee directly, which is why it was engaging the former employee through Coupang and providing Coupang with specific instructions on what to say and how to interact with him.[211] On December 10, 2025, Park Dae-jun resigned and Coupang Inc.'s General Counsel and Chief Administrative Officer, Harold L. Rogers, was named as interim CEO of Coupang Corp.[212]

When the former employee responded to Coupang on December 11, 2025, NIS provided Coupang with a list of questions to ask him.[213] Between December 11 and December 16, Coupang communicated with the disgruntled former employee through their respective attorneys on multiple occasions, keeping NIS informed of each exchange and receiving guidance on how to proceed, before ultimately arranging an in-person meeting.[214]

During these discussions, Coupang's legal team was able to secure a confession from the former employee and confirm that the devices he used to store data were located in Shanghai, China.[215] These devices included four hard drives, a desktop computer, and a graphics card that were still in the former employee's possession as well as a laptop computer that he had discarded in a local river shortly after the unauthorized access was announced to the public.[216] With the

---

[206] *Id.*
[207] *Id.*
[208] CPNG-HJC119-0000887, at 989-90; CPNG-HJC119-0001070, at 1080-81; CPNG-HJC119-0001549, at 1569-71; CPNG-HJC119-0002056; CPNG-HJC119-0002057, at 2059.
[209] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 98-99; CPNG-HJC119-0001070, at 1081; CPNG-HJC119-0001549, at 1571; CPNG-HJC119-0002057, at 2059.
[210] *See* CPNG-HJC119-0001070, at 1081; CPNG-HJC119-0002057, at 2059; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 100.
[211] *See* CPNG-HJC119-0001070, at 1081; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 100.
[212] *See* CPNG-HJC119-0001509, at 1524; CPNG-HJC119-0001592.
[213] *See* CPNG-HJC119-0001070, at 1081-82; CPNG-HJC119-0002057, at 2059; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 129.
[214] *See* CPNG-HJC119-0001070, at 1081-83; CPNG-HJC119-0002056; CPNG-HJC119-0002057, at 2059-61; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 129-30.
[215] *See* CPNG-HJC119-0001070, at 1081-83; CPNG-HJC119-0001549, at 1576; CPNG-HJC119-0002057, at 2059-61; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 129-30.
[216] *See* CPNG-HJC119-0000836, at 846; CPNG-HJC119-0000887, at 1017; CPNG-HJC119-0002057, at 2061; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 133.

exception of the laptop that was no longer in his possession, on December 15, 2025, the former employee brought each of the devices to the Shanghai headquarters of Han Kun Law Offices, a multinational law firm retained by Coupang in connection with this matter.[217] The following day, after Coupang informed NIS that its lawyers had secured the devices, NIS told Coupang that as a foreign intelligence agency, it could not operate in China, and that Coupang would need to send one of its own employees to retrieve the devices.[218]

Mr. Rogers testified that he initially decided "the risk" of sending a Korean employee to China to retrieve the devices "was too high," but was once again "told that, under Korean law" Coupang was "required to" comply with NIS's instructions.[219] He stated that he "never would have allowed one of [Coupang's] Korean employees to go to China to basically operate as an NIS operative on Chinese soil unless [he] believed that it was required of [Coupang] by law."[220] Nonetheless, Coupang continued to express concerns about the operation, and NIS eventually agreed to have personnel "nearby" for safety reasons, though the agency made it clear that a Coupang employee would ultimately need to retrieve the devices as well as sworn statements from the disgruntled former employee without NIS's involvement.[221]

On December 16, 2025, Coupang raised additional concerns about continuing with the operation without first notifying the police.[222] NIS responded "that, given the high risks involved in the retrieval operation, it would be best not to notify the police until the retrieval was complete to ensure a safe and successful operation."[223] Coupang spoke with NIS officials dozens of times on December 16 to finalize the details of the recovery operation, such as where the hand-off would occur and what the former employee should say in his sworn statement.[224] During these discussions, NIS provided detailed advice and recommendations to Coupang on how the operation should proceed.[225]

The following day, December 17, 2025, Arthur flew to Shanghai and then traveled to the Han Kun Law Offices to retrieve the devices and sworn statements.[226] In these statements, the former employee confirmed that he had used a stolen key to access customer data, that the data he accessed did not include high-sensitivity information, and that he no longer possessed or controlled any data or information that belong to Coupang or its users.[227]

---

[217] *See* CPNG-HJC119-0000836, at 846; CPNG-HJC119-0002057, at 2060-61.
[218] *See* CPNG-HJC119-0001070, at 1083; CPNG-HJC119-0001509, at 1536; CPNG-HJC119-0002057, at 2061; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 131.
[219] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 131; CPNG-HJC119-0001597, at 1616; *see also* CPNG-HJC119-0002057, at 2061.
[220] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 131; CPNG-HJC119-0001597, at 1618.
[221] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 132; CPNG-HJC119-0000887, at 996-1008.
[222] *See* CPNG-HJC119-0001070, at 1083; CPNG-HJC119-0002057, at 2061.
[223] CPNG-HJC119-0001070, at 1083; CPNG-HJC119-0002057, at 2061; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 131.
[224] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 131-32; CPNG-HJC119-0001070, at 1083-84; CPNG-HJC119-0002056; CPNG-HJC119-0001070, at 1083; *see also* CPNG-HJC119-0002057, at 2061.
[225] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 131-32; CPNG-HJC119-0001070, at 1083-84; HJC119-0002056; CPNG-HJC119-0002057, at 2061.
[226] *See* CPNG-HJC119-0001070, at 1084; CPNG-HJC119-0002057, at 2061; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 132-33.
[227] *See* CPNG-HJC119-0000833, at 835; CPNG-HJC119-0000836, at 845-48.

Mr. [redacted] Statement

1. I previously worked as a backend engineer at Coupang Corp., and my employment relationship with Coupang terminated in December 2024.
2. In 2025, I obtained some Coupang user data. The Coupang data I obtained did not contain any users' bank information, credit card information, or login credentials.
3. My purpose in obtaining this data is to reveal a specific vulnerability in Coupang's security system. I did not obtain this data for sale, transfer, or any other purpose; it is solely intended to alert Coupang to this security vulnerability.
4. In November 2025, I sent an email to Coupang and some Coupang users informing them of the data security vulnerability. Apart from the aforementioned email, I have not disclosed, sold, transferred, or shared any Coupang user data, or confidential information of Coupang and its users, to any individual or entity outside of Coupang.
5. After my actions were made public, I immediately deleted all Coupang user data. I no longer hold or control any Coupang user data.
6. On December 9, 2025, I was contacted by Coupang regarding user data that Coupang believes I hold.
7. I no longer possess, store, or control any data, information, or files belonging to Coupang or its users. I also no longer own the computer device that was used to store Coupang user data. However, as stated above, I previously deleted all Coupang data from that computer device, therefore the device no longer contains any Coupang data.
8. I hereby declare that the above content is true and accurate, and I am willing to bear legal responsibility for any false statements.

[redacted]

[redacted]

Page 1 of 1

[redacted]

CONFIDENTIAL TREATMENT REQUESTED
NOT FOR DISTRIBUTION
MEMBERS & STAFF ONLY

CPNG-HJC119-0000835

Translation of one of former employee's sworn statements regarding the unauthorized access.[228]

[228] CPNG-HJC119-0000833, at 835

According to Mr. Rogers' testimony and documents produced to the Committee and Subcommittee, after Arthur took possession of the materials, NIS told Arthur to go to a private location where there were "no CCTV cameras to capture the hand off" to NIS.[229] Arthur then gave the equipment and statements to an NIS official, who "immediately departed for the Korean Embassy in Shanghai."[230] The next morning, NIS instructed Arthur to contact the former employee again in order to get his fingerprints on each of the sworn statements.[231] NIS also asked that Coupang hire divers to search for the former employee's laptop in the river where he disposed of it.[232]

That same day, Coupang did as it was ordered. Coupang's divers retrieved the laptop from the river and reported this to NIS.[233] Additionally, Arthur took the sworn statements back from NIS, had the former employee put his fingerprints on them, and delivered both the statements and the laptop to an NIS official in the same location they had met the previous day.[234] The NIS official then returned to the Korean Embassy in Shanghai, and NIS transported the evidence back to South Korea in a diplomatic pouch the following day.[235] On December 21, Coupang submitted copies of the devices and explained the details of the NIS-directed recovery operation to the police.[236] By December 23, 2025, Coupang had provided these same materials to both the Joint Investigations Team and the PIPC and fully briefed them on the details of the recovery operation.[237] On December 25, Coupang announced the results of the recovery operation to the public.[238]

Despite the fact that NIS initiated and was substantially involved in the recovery operation, on December 26, 2025, NIS issued a press release stating that the agency "ha[d] issued no instructions" to Coupang regarding the operation.[239] However, as demonstrated above, this is directly contradicted by documents and testimony obtained by the Committee and Subcommittee.

Documents produced to the Committee and Subcommittee show that between December 1 and December 26, NIS had over 230 phone calls and several in person meetings with Coupang to discuss the former employee's unauthorized access of Coupang's data systems and to plan the recovery effort.[240] Throughout these conversations, NIS "instruct[ed] [Coupang] on what to do"

---

[229] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 133; CPNG-HJC119-0001597, at 1614.
[230] CPNG-HJC119-0001070, at 1084.
[231] *See* CPNG-HJC119-0001070, at 1085; HJC119-0002056; CPNG-HJC119-0002057, at 2062.
[232] *See* CPNG-HJC119-0001070, at 1085; HJC119-0002056; CPNG-HJC119-0002057, at 2062; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 133.
[233] *See* CPNG-HJC119-0001070, at 1085; CPNG-HJC119-0002057, at 2062; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 133.
[234] *See* CPNG-HJC119-0001070, at 1085; CPNG-HJC119-0002057, at 2062; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 133.
[235] *See* CPNG-HJC119-0001070, at 1086; CPNG-HJC119-0002057, at 2062; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 133-34.
[236] *See* CPNG-HJC119-0000887, at 893; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 134.
[237] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 134; CPNG-HJC119-0000455, at 573.
[238] *See* Heejin Kim, *Coupang says all leaked customer information has been deleted*, REUTERS (Dec. 25, 2025).
[239] CPNG-HJC119-0000869, at 870.
[240] *See* CPNG-HJC119-0001070, at 1079-87; CPNG-HJC119-0002056; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 133-34.

and provided "directions" on the actions that Coupang should take, down to the "specific content and tone" that Coupang should use in emails to the disgruntled former employee.[241] NIS also repeatedly directed Coupang not to discuss the recovery operation with the police or other government agencies.[242] NIS did not suggest that Coupang was free to ignore its requests a single time throughout these discussions.[243] In fact, "NIS consistently made it very clear that [Coupang] w[as] required to comply with their instructions."[244] NIS even provided Coupang with a formal document citing the "Relevant Legal Basis" for this requirement.[245] According to Mr. Rogers, he "never would've authorized an employee to go to China" or "authorized hiring a diving crew in broad daylight in China to retrieve a device unless [he] firmly believed that [Coupang] had a legal obligation and a requirement to do so."[246]

In addition, documents produced pursuant to the subpoena show that a high-ranking official within South Korea's Presidential Office had specifically "instructed" Coupang to work closely with NIS in order to recover the devices from the former employee and deliver them to NIS.[247] On December 12, a Coupang employee spoke with the official "to discuss appropriate measures to take in response to the data leak" and "agreed that it was important for both Coupang and the government to work together collaboratively in the interest of information security and national security for the people of Korea."[248] On December 15, Coupang told the official "that personnel had acquired the suspect's desktop PC and hardrives in Shanghai in coordination with the NIS" and "discussed appropriate steps to ensure the devices were returned safely to Korea."[249] During this conversation, the official said that "he would brief President Lee Jau-myung."[250] The following day, the official "confirmed that he had briefed President Lee Jae-myung about [the] acquisition and recovery of the devices" and once again told Coupang to "follow NIS instructions."[251] On December 19, 2025, the Coupang employee messaged the official to confirm that the company had successfully recovered all of the data as directed by the NIS.[252]

As these documents indicate, the highest levels of the South Korean government, including President Lee Jau-myung himself, knew that NIS had been closely instructing Coupang on the recovery operation and that Coupang acted in response to these directives.[253]

---

[241] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 135; CPNG-HJC119-0001597, at 1612-13; CPNG-HJC119-0002056; CPNG-HJC119-0002057.
[242] *See* CPNG-HJC119-0001070, at 1079-83; CPNG-HJC119-0000887, at 964, 966; CPNG-HJC119-0002057; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 93, 97-100, 131.
[243] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 97, 135-36; CPNG-HJC119-0001070, at 1080; CPNG-HJC119-0002057.
[244] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 135; CPNG-HJC119-0001597, at 1613-14; CPNG-HJC119-0002057.
[245] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 135; CPNG-HJC119-0001597, at 1613-14; CPNG-HJC119-0002057.
[246] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 136.
[247] CPNG-HJC119-0002057, at 2060-63.
[248] CPNG-HJC119-0002057, at 2060.
[249] CPNG-HJC119-0002057, at 2060-61.
[250] CPNG-HJC119-0002057, at 2061.
[251] CPNG-HJC119-0002057, at 2061.
[252] *See* CPNG-HJC119-0002057, at 2062.
[253] *See id.*.

The South Korean government knew that the scope of the unauthorized access was far narrower than was being reported.[254] Despite this knowledge, the South Korean government continued to publicly attack Coupang and spread misleading information about the company anyway.[255]

3. The National Assembly Hearings

On December 30 and December 31, 2025, Mr. Rogers and other Coupang executives testified before a joint session of six committees in the South Korean National Assembly.[256] In these hearings, members of the National Assembly demonstrated the openly hostile and discriminatory manner in which the South Korean government treats American-owned companies.[257] Rather than asking substantive questions about the nature and scope of the former employee's unauthorized access of Coupang's data systems, National Assembly members insulted and berated Coupang's employees, called for Coupang to be bankrupted, lied about the unauthorized access and recovery operation, and even pressed for criminal charges to be brought against Coupang's executives, including American citizens.[258]

When asked about the National Assembly hearings, Mr. Rogers testified to the Committee and Subcommittee that he was "compelled to appear under threat of criminal prosecution," and that the hearings were overtly adversarial.[259] During the hearings, Mr. Rogers' interpreter was "told that she could not interpret [his] answers" and "the chairwoman ridiculed her for being there," saying that she "was doing a terrible job" and should "only interpret the things that the chairwoman wanted to hear."[260] Instead, the National Assembly forced Coupang's executives to use an interpreter that it had selected.[261] According to Mr. Rogers, the National Assembly's interpreter "did not provide . . . full and complete translations of what was being asked."[262] Mr. Rogers explained that he "wasn't given the opportunity to have those interpretations finalized or redone when [he] had questions" and was "shown documents in Korean that were not translated for" him.[263] Even more, the National Assembly denied Mr. Rogers the ability to have his U.S. counsel attend the hearings with him.[264]

---

[254] *See* CPNG-HJC119-0001067; CPNG-HJC119-0001488; CPNG-HJC119-0001730; CPNG-HJC119-0001738; CPNG-HJC119-0002057.
[255] *See* CPNG-HJC119-0001067; CPNG-HJC119-0001488; CPNG-HJC119-0001730; CPNG-HJC119-0001738; CPNG-HJC119-0002057.
[256] *See* CPNG-HJC119-0000455; CPNG-HJC119-0000631; CPNG-HJC119-0001597, at 1604-07; CPNG-HJC119-0002057 Deposition of Mr. Harold L. Rogers, *supra* note 15, at 136.
[257] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 128-40; CPNG-HJC119-0000455; CPNG-HJC119-0000631; CPNG-HJC119-0001597, at 1604-07.
[258] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 128-40; CPNG-HJC119-0000455; CPNG-HJC119-0000631; CPNG-HJC119-0001597, at 1604-07.
[259] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 136-38; CPNG-HJC119-0001597, at 1604-07.
[260] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 136-38; *see also* CPNG-HJC119-0001711.
[261] *See id.* at 136; CPNG-HJC119-0001711.
[262] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 136-37; CPNG-HJC119-0001597, at 1604-07; CPNG-HJC119-0001711.
[263] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 136-37; CPNG-HJC119-0001597, at 1604-07; CPNG-HJC119-0001711.
[264] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 137.

Throughout the proceedings, Mr. Rogers "was often not allowed to answer questions" that were asked by members of the National Assembly.[265] He was "threatened with perjury," "threatened with arrest," "threatened with a travel ban," and "threatened with deportation."[266] In fact, Mr. Rogers was "threatened with personal criminal action more than 20 times" on the first day of the hearing alone.[267] Mr. Rogers told the Committee and Subcommittee that he "was sworn at, called a liar, [and] called . . . the equivalent in Korean of a mother F'er in the hearing."[268] In addition, "[s]everal National Assemblymen called for [Coupang] to be bankrupted" and "asked for the passage of a Coupang law to put [the company] out of business."[269]

National Assembly members also "called [Coupang] an organized crime organization or a mafia on multiple occasions," and a member even told the Acting Commissioner of the National Police Agency that he needed to "conduct [a] search and seizure, investigate immediately, and punish [Coupang]."[270] One member of the National Assembly displayed his phone screen on camera during the hearing, canceled his Coupang membership, and encouraged his fellow Korean citizens to cancel their memberships as well and sign up for one of Coupang's Korean competitors.[271] Korean officials even went as far as to refer to Coupang's Founder and Chief Executive Officer, Bom Kim, as a "dark-haired foreigner," a derogatory term for someone who was born in Korea but has since become a citizen of another country.[272]

When a member of the National Assembly asked Mr. Rogers about the recovery operation, he testified that Coupang "did not conduct an investigation on [its] own, but investigated according to the instructions of the government."[273] Mr. Rogers explained that NIS had told Coupang that it "needed to cooperate," and based on South Korean law, Coupang "understood that [it] had to follow this agency's instructions."[274] He testified that NIS "told [Coupang] to contact the suspect," and that Coupang had made copies of the former employee's devices based on "an instruction from . . . the government agency."[275] Mr. Rogers explained that the entire recovery operation was "conducted according to government instructions."[276]

In response to Mr. Rogers' testimony, a member of the National Assembly "conveyed that the NIS plan[ned] to request the National Assembly . . . file a complaint against Harold Rogers, CEO of Coupang for perjury."[277] A different member said that the National Assembly "must file a criminal complaint about this," and that "an immediate travel ban on CEO Harold Rogers is necessary" to prevent him from leaving the country.[278] Later that day, NIS issued a

---

[265] *Id.*
[266] *Id.*
[267] CPNG-HJC119-0000455, at 476.
[268] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 137.
[269] *Id.* at 140.
[270] *Id.*; CPNG-HJC119-0000631, at 695-96.
[271] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 140.
[272] *Id.* at 128-29;
[273] CPNG-HJC119-0000631, at 700.
[274] *Id.* at 701-02.
[275] *Id.* at 702.
[276] *Id.* at 704.
[277] *Id.* at 752.
[278] *Id.* at 795-96.

public statement insisting that Mr. Rogers' claims were "entirely untrue" and that "NIS has never issued any instructions, orders or authorization to Coupang, nor is it in a position to do so."[279] NIS also filed an official request asking "that the National Assembly charge Coupang interim CEO Harold Rogers with perjury over claims that the NIS meddled in the corporate investigation into a recent data leak."[280]

I, [redacted] certify that I am competent to translate from Korean into English and that the translation below of the NIS press release is true, accurate, and complete to the best of my knowledge. This translation has been reviewed and verified by a human translator. If you have any questions regarding the translation, please contact me via the email address below.

Typed Name: [redacted]
Qualifications: Professional Translator with an MA in Translation, Seoul, Korea
Email: [redacted]@coupang.com
Date: February 4, 2026

[Translation of the NIS press release]

[Letterhead of the NIS] Press release

Tel. 02-2210-8007
December 30, 2025

The National Intelligence Service ("NIS") Requests the National Assembly to File a Criminal Complaint against Coupang's CEO for Perjury.

- The series of statements by Coupang's CEO, including those regarding "investigation instructions from the NIS", are obviously false.

The NIS hereby clarifies its position concerning the demonstrably false statements made by the CEO of Coupang while responding to questions from some committee members during the "joint hearing" of six standing committees held at the National Assembly on December 30.

First, Coupang CEO's claim that "Coupang did not conduct its investigation independently, but according to the instructions and order of the NIS" is entirely untrue.

Aside from requesting materials, the NIS has never issued any instructions, orders or authorization to Coupang, nor is it in a position to do so.

Second, the claim that "Coupang did not wish to contact the leaker, but the NIS ordered such contact and communication" is also untrue.

On the contrary, in response to Coupang's request for our opinion on "contacting the leaker," the NIS emphasized multiple times that "it would be appropriate for Coupang to make the final judgment."

Third, the claim that "forensic images of the hard drives were also taken as per the instructions of a government agency" is also untrue.

Prior to the time when the NIS contacted Coupang on site to facilitate the secure transport of IT equipment already retrieved by Coupang from the leaker (*i.e.*, December 17), Coupang had already independently duplicated the copies of the images (*i.e.*, December 15), and the NIS was completely unaware of this until its contact with Coupang on December 17.

CONFIDENTIAL TREATMENT REQUESTED
NOT FOR DISTRIBUTION
MEMBERS & STAFF ONLY CPNG-HJC119-0000439

Translation of the official request to file a criminal complaint against Mr. Rogers.[281]

[279] CPNG-HJC119-0000439; CPNG-HJC119-0000416, at 416-17.
[280] CPNG-HJC119-0000413; CPNG-HJC119-0000435-36.
[281] CPNG-HJC119-0000437, at 439.

On December 31, 2025, the National Assembly responded to NIS's request and decided to file criminal complaints against Mr. Rogers and seven other current and former executives from Coupang.[282] On January 16, 2026, the National Assembly's Science, ICT, Broadcasting, and Communications Committee officially filed a criminal complaint against Mr. Rogers on charges of perjury for the statements he made about NIS during the hearings.[283] On January 30, 2026, South Korean police interviewed Mr. Rogers for 12 hours regarding the former employee's unauthorized access and his testimony at the National Assembly hearings.[284] Police interviewed Mr. Rogers again on February 6 for an additional 14 hours.[285] Notably, on February 12, 2026, the National Assembly passed the Personal Information Protection Act, commonly referred to as the "Anti-Coupang Act," which specifically targets Coupang and would subject companies to a fine of up to 10 percent of their revenue for certain types of information leaks.[286]

4. The South Korean Government's Retaliation against Coupang

Following the former employee's unauthorized access of Coupang's data systems, the South Korean government has initiated dozens of investigations across multiple different agencies, many of which are entirely unrelated to the data breach.[287] In fact, of the 40 different investigations launched by South Korea since November 2025, 33 are unrelated to the former employee's unauthorized access of Coupang's data systems.[288] One Korean reporter compared it to a "Korean proverb about burning down a thatched house to kill a flea," noting that over ten different government agencies have deployed hundreds of investigators to conduct onsite inspections of the company.[289] Overall, since the data incident, the South Korean government has issued 4,229 document requests to Coupang and conducted 652 separate interviews involving over 600 different employees.[290] According to Mr. Rogers, this was "done as a response from [the South Korean] President telling the agencies to directly attack" Coupang.[291]

In one example, South Korean regulators had already "summarily dismissed" a severance-related issue "over 77 times by the labor ministry before [Coupang's] data leak," and prosecutors had consistently determined that there had been "no violation of the law."[292] However, Mr. Rogers testified that "[o]nce this data leak became an issue and there was directive from the President and the Prime Minister to go after Coupang in any and every way possible, . . . then all of a sudden [government officials] showed up . . . at [Coupang's] offices and started seizing documents."[293] Although numerous agencies and multiple prosecutors had already determined that Coupang had not violated the law, after the data incident, two of Coupang's executives were personally indicted and subjected to travel bans and the threat of prison time

[282] *See* CPNG-HJC119-0000876, at 876-77; CPNG-HJC119-0001065, at 1065-66.
[283] *See* CPNG-HJC119-0000440, at 440-54.
[284] *See* Deposition of Mr. Harold L. Rogers, *supra* note 15, at 146-47.
[285] *See* CPNG-HJC119-0001732; Deposition of Mr. Harold L. Rogers, *supra* note 15, at 146-47.
[286] *See* CPNG-HJC119-0001743; CPNG-HJC119-0001740.
[287] *See* CPNG-HJC119-0001736.
[288] *See* CPNG-HJC119-0001994.
[289] *Investigation of Coupang Must Balance Enforcement with Efficiency*, UNITED PRESS INTERNATIONAL (Jan. 27, 2026).
[290] *See* CPNG-HJC119-0001994.
[291] Deposition of Mr. Harold L. Rogers, *supra* note 15, at 155.
[292] *Id.* at 113-15.
[293] *Id.*

over this issue.[294] These threats are made even more troubling by the fact that South Korean prosecutors have a conviction rate of close to 99 percent.[295]

After South Korea launched its campaign against the company, Coupang's market capitalization fell by more than 40 percent.[296] This decrease has negatively affected U.S. investors, including public pension funds, mutual funds, and everyday Americans just trying to save for retirement.[297] The South Korean government's coordinated attacks on Coupang have also harmed other American businesses and producers, which sell billions of dollars' worth of products through Coupang's online platform every year.[298] As mentioned above, on June 11, 2026, South Korea fined Coupang over $410 million, the largest fine ever imposed on a single company.[299] This fine is substantially larger than those imposed on South Korean companies for more serious data breaches involving highly sensitive personal information.[300]

The discriminatory nature of the South Korean government's actions against Coupang following the data breach and its impact on Americans has already received considerable attention in the United States. On January 22, 2026, two of Coupang's largest investors filed a petition with the Office of the United States Trade Representative (USTR) under Section 302(a) of the Trade Act of 1974.[301] In this petition, the investors asked the USTR to "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."[302] The petition states that "[t]he Korean Government is currently in the midst of a whole-of-government assault on Coupang," and that it is "unjustifiably and arbitrarily singling out Coupang for discriminatory treatment and disproportionate punishment."[303] On March 9, 2026, the investors withdrew this petition after the Trump Administration signaled its willingness to launch a broader investigation into South Korea's discriminatory treatment of American-owned companies.[304]

Several other United States officials and Members of Congress have also raised concerns about South Korea's discriminatory attacks on Coupang. In addition to the investigation launched by the Committee and Subcommittee, on April 20, 2026, fifty-four Members of Congress sent a letter to South Korea demanding that it stop targeting American-owned businesses, citing "[t]he systematic targeting of American companies such as Apple, Google, Meta, and Coupang."[305] In addition, Vice President JD Vance warned South Korea's Prime

---

[294] *See id.*
[295] *See* Yoo Hee-kon, *First-Instance Acquittal Rate Exceeds 1% for First Time*, CHOSUN DAILY (Feb. 9, 2026).
[296] *See Coupang, Inc. (CPNG)*, YAHOO FINANCE (last visited May 20, 2026).
[297] *See* CPNG-HJC119-0001673; *U.S. investment firms take legal action against South Korea over Coupang*, INVESTING (Jan. 22, 2026).
[298] *See* CPNG-HJC119-0001673, at 1680.
[299] Jun, *supra* note 26.
[300] Gyu-lee, *supra* note 26.
[301] *See* CPNG-HJC119-0001673.
[302] *Id.* at 1675.
[303] *Id.*
[304] *See* Ari Hawkins, *US investors withdraw Korea trade petition as USTR eyes broader probe*, POLITICO (Mar. 9, 2026).
[305] Letter from Rep. Michael Baumgartner et al. to the Hon. Kyung-wha Kang, Ambassador to the United States of America, Republic of Korea (Apr. 20, 2025)

Minister Kim Min-seok against targeting innovative American technology companies, including Coupang, amid ongoing trade tensions between the United States and South Korea.[306] Such practices likely violate the Trump Administration's recent trade agreement with South Korea, which specifically provides that South Korea must "ensure that U.S. companies are not discriminated against and do not face unnecessary barriers in terms of laws and policies concerning digital services, including . . . online platform regulations."[307]

III. CONCLUSION

The South Korean government has a long history of discriminating against American-owned businesses. The KFTC has played a central role in this discrimination, using burdensome obligations, aggressive enforcement practices, and even the threat of criminal penalties to punish U.S. companies and prevent them from successfully competing against their Korean rivals. South Korea has even weaponized digital laws and regulations to attack American companies and limit their ability to operate in the South Korean market.

Coupang, an innovative American e-commerce company, has been a consistent target of the South Korean government. South Korea has subjected Coupang to ceaseless investigations, unjustifiable production demands, and has even threatened to suspend the company's business operations. While South Korea's hostility toward Coupang has been going on for years, it has escalated considerably after a former employee stole a limited amount of customer data from Coupang.

Following this incident, the South Korean government had spread false information about Coupang, referred to it as a criminal organization, and launched numerous investigations into the company, many of which are entirely unrelated to the incident itself. Even worse, after forcing Coupang to engage in a dangerous recovery operation that involved sending an employee to China and retrieving devices and sworn statements from the former employee, South Korea lied about its involvement in the operation and threatened Coupang's CEO, an American citizen, with criminal charges. American businesses, government officials, and U.S. investors have all raised concerns about South Korea's discriminatory behavior against Coupang.

The Committee on the Judiciary is entrusted with the "[p]rotection of trade and commerce against unlawful restraints and monopolies."[308] This report documents South Korea's history of discriminatory behavior toward American-owned businesses and its recent attacks on an innovative U.S. company, including its threats to bring criminal charges against an American citizen. South Korea's conduct is part of a broader attempt by foreign governments to weaponize their laws and regulations in an effort to harm American companies and limit their ability to compete in the global economy. Such conduct demonstrates how competition laws and other regulatory frameworks designed or applied without principled limitations and due process protections can be used as an instrument of economic coercion against American-owned businesses. The Committee and Subcommittee will continue its oversight to inform legislative reforms to better protect American business and consumers.

[306] *See* Bade & Ramkumar, *supra* note 109.
[307] White House, *supra* note 28.
[308] Rules of the House of Representatives R. X (2025).