COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT
JOHANNESBURG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Marney L. Cheek

Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5267
mcheek@cov.com

January 22, 2026

His Excellency Mr. Lee Jae Myung
President of the Republic of Korea
Cheong Wa Dae
1 Cheongwadae-ro, Jongno-gu
Seoul 03048
Republic of Korea

His Excellency Mr. Hong-Sik (Justin) Chung
Deputy Minister
Office of International Legal Affairs
Ministry of Justice of the Republic of Korea
Government Complex, Gwacheon
Republic of Korea

Re: Notice of Intent to Bring Arbitration Claims Against the Republic of Korea for Violations of the United States-Korea Free Trade Agreement

Your Excellencies:

We represent the U.S. investment firm Greenoaks Capital Partners LLC ("Greenoaks") and various investment funds that Greenoaks manages; Mr. Neil Mehta and Mr. Benjamin Peretz, the founders and managing partners of Greenoaks; and the U.S. investment firm Altimeter Capital Management, LP ("Altimeter") and various investment funds that Altimeter manages (collectively, the "U.S. Investors").

We write to provide notice that the U.S. Investors intend to file arbitration claims against the Republic of Korea pursuant to the Free Trade Agreement between the United States of America and the Republic of Korea (the "Treaty"), based on the Government's discriminatory, disproportionate, and pretextual attacks on the U.S. technology and online retail company Coupang Inc., and its wholly owned Korean subsidiary Coupang Corp. (collectively, "Coupang"). Coupang has been publicly traded on the New York Stock Exchange (the "NYSE") since 2021. The U.S. Investors own shares of Coupang worth more than $1.5 billion.

Overwhelming evidence establishes that the Government is using the pretext of a limited data breach at Coupang perpetrated by a Chinese threat actor, which the company appears to have fully rectified, to try and eliminate a successful U.S. company's ability to compete with the Korean and Chinese companies that the Government favors.

To date, the Government's illegal actions have erased billions of dollars of U.S. investment in Coupang. Recently, the Government has threatened to suspend Coupang's

business license and bankrupt the company. The President of Korea, Mr. Lee Jae Myung ("President Lee"), has explicitly stated that Coupang should face penalties so severe that it fears collapse. If the Government follows through on these threats, it will erase tens of billions of dollars more of U.S. investment.

The Government's unprecedented assault on a U.S. company to benefit its Korean and Chinese competitors is an egregious violation of the Treaty, principles of international law, and the historic partnership between Korea and the United States, which has lasted more than 75 years. It is something that U.S. investors might expect from totalitarian adversaries like Venezuela or Russia; it is not something they could have imagined happening in a representative democracy, advanced economy, and critical ally like Korea.

The U.S. Investors have deep affinity and respect for Korea and its people and have no desire to bring these claims. Indeed, in the 14 years since Greenoaks was founded, and the 18 years since Altimeter was founded, across the more than $30 billion of assets they manage, they have never brought any legal action of any kind against any individual, entity, or state.

But the Government's shocking conduct has left the U.S. Investors with no choice. If the Government does not immediately cease its attacks against Coupang, fully restore the company's ability to operate its business, and permanently end its longstanding campaign of discrimination against the company, then the U.S. Investors will be forced to seek billions of dollars in damages from Korea to protect their investments in Coupang and remedy the Government's ongoing Treaty violations, including attempted expropriation.

I. Factual Background

A. Coupang Creates Tremendous Value for U.S. Investors, Korean Consumers, and Korean Workers

Coupang is one of the great success stories of the special relationship between the United States and Korea. As Korea's largest online retail company, Coupang is often referred to as the "Amazon of South Korea." In the 16 years since it was founded, Coupang has created tremendous value for U.S. investors, Korean consumers, and Korean workers alike.

Generally, U.S. investors, including investment firms, public pension funds, and individual shareholders, have benefited as Coupang generated impressive revenues and joined the Fortune 150. In 2024, the most recent year for which full financial data is available, Coupang reported revenue of over $30 billion. As recently as September 2025, the company reached a market capitalization of $60 billion. U.S. investors own the vast majority of Coupang's stock.

Korean consumers benefited as Coupang revolutionized e-commerce in the country by offering unparalleled value, selection, and speed for the products that are sold on its platforms. Coupang unlocked these benefits for Korean consumers in part by building a proprietary logistics network from the ground up. This network comprises more than 100 fulfillment and logistics centers, advanced automation and software systems, and a fleet of over 25,000 delivery vehicles operating nationwide.

As a result, Coupang has become beloved in Korea—many Koreans happily report that they could not live without Coupang. The company is especially well-known for its "Dawn Delivery" service, through which it guarantees next-morning delivery for orders placed by midnight. For young Korean parents who run out of diapers, or elderly Korean grandparents who run out of groceries, Coupang is often a lifesaver.

In a virtuous cycle, it was billions of dollars of U.S. investment in Coupang that enabled the company to develop and deploy the cutting-edge technologies that unlocked the best prices, widest variety, and fastest deliveries for Korean consumers. Delighted by Coupang's offerings, Korean consumers bought more products through the company, which increased the company's revenues, profits, and valuation, and grew the pensions and retirement accounts of workers in the United States who owned Coupang stock.

Korean employees have benefited too. Coupang is the second-largest employer in Korea, and has created more than 100,000 jobs in the country. The company has also invested billions of dollars in Korean infrastructure, indirectly creating many thousands of additional jobs.

As this positive feedback loop accelerated, Coupang began taking significant market share from large, established Korean conglomerates. These firms were unaccustomed to competition from innovative entrants in their markets, especially U.S. ones. Coupang also began taking market share from enormous Chinese conglomerates operating in Korea that maintain close ties with the People's Republic of China, the Democratic Party of Korea (the "DPK"), and President Lee.

Once it became clear that Coupang was threatening the historical dominance of its Korean and Chinese competitors, the Government began weaponizing the administrative power of the state, and even acting outside its sovereign capacity, to disrupt Coupang's operations.

B. The Government Targets Coupang to Protect Its Entrenched Korean and Chinese Conglomerate Competitors

For years, the Government has deployed a broad array of Korean agencies against Coupang, all working in concert with each other, including the Korea Fair Trade Commission (the "KFTC"), the Ministry of Employment and Labor (the "MOEL"), the Financial Supervisory Service (the "FSS"), and the National Tax Service (the "NTS").

Over the past several years especially, as the threat Coupang poses to its Korean and Chinese competitors has increased, the Government's harassment of Coupang has correspondingly intensified. For example, the KFTC opened three investigations of Coupang in 2021, five in 2022, seven in 2023, ten in 2024, and nine in 2025.

This trend was as true across the Government as it was for the KFTC. In 2024 and 2025, Coupang and its affiliates were audited, inspected, and raided by Government agencies hundreds of times.

During this same period, the Government appears to have subjected Coupang's main Korean and Chinese competitors to extremely limited enforcement actions, even though these companies followed many of the same business practices that the Government scrutinized at Coupang.

To pick one illustrative example among these hundreds, the KFTC investigated Coupang for years under the Monopoly Regulation and Fair Trade Act (the "MRFTA") for allegedly using its search algorithms and other methods to boost its own products. At the conclusion of the KFTC's investigation in June 2024, it imposed a fine of over $100 million against Coupang, the largest fine ever imposed against a retail company in Korea, and filed a criminal complaint against the company with the Prosecutor's Office.

But when the KFTC investigated Naver, one of Coupang's main Korean competitors, under the MRFTA for altering search algorithms to favor its own products, it imposed a fine of only $23 million, and did not make any criminal referral. By October 2025, even before the data breach discussed in this letter, the KFTC had already imposed more penalties against Coupang than against any other company in Korean history.

As noted, the KFTC's $100 million fine is merely one example of a discriminatory, disproportionate, and pretextual Government action against Coupang. Others abound. If the U.S. Investors are ultimately forced to bring arbitration claims against Korea, they are prepared to introduce extensive evidence of numerous other examples of Government action against Coupang that had no basis in law or fact, along with examples of competitors who engaged in similar conduct without any Government scrutiny, or which resulted in dramatically lower penalties.

For years, these illegal Government actions against Coupang were a persistent impediment. But starting in 2025, they became an existential threat, when President Lee's election gave the DPK a unified government for the first time since 2022.

President Lee is a polarizing figure in Korea, even among his supporters, due in part to concerns that he will reorient Korea economically, politically, and militarily away from the United States—its enduring ally since World War II—and toward an increasingly aggressive China committed to regional hegemony. Based on President Lee's actions since he took office, these concerns have only increased.

From the beginning of President Lee's campaign for the presidency, he has made many statements that are hostile toward the United States generally and Coupang specifically. For example, President Lee called U.S. troops stationed in Korea an "occupying force," and "blamed the U.S. for maintaining Japan's colonization of Korea." These statements are in keeping with the DPK's increasingly anti-U.S., pro-China stance.

In addition to his ideology, President Lee has also appointed senior officials with significant prior ties to Coupang's competitors, creating strong incentives to hurt Coupang. By late 2025, President Lee's cabinet included two ministers who are former CEOs of a major Coupang competitor: Han Seongsook, currently the Minister of Small and Medium Enterprises, and Startups, and formerly the CEO of Naver; and Chae Hwi-young, currently the Minister of

Culture, Sports and Tourism, and previously the CEO of Naver's former parent company NHN and a Naver advisor. Additionally, President Lee's Senior Secretary for AI Future Planning, Ha Jung-woo, formerly served as the head of Naver's AI Innovation Center.

Thus, for both ideological and more pragmatic reasons, President Lee was primed to use the first available pretext to attack Coupang. President Lee seized his opportunity late last year, when Coupang was the victim of a limited data breach perpetrated by a Chinese former employee based in China.

C. A Chinese Threat Actor Perpetrates a Limited Data Breach at Coupang

Some of the best evidence of the Government's illegal efforts to destroy Coupang comes from comparing the objective facts of the limited data breach with what the Government falsely claims happened. The Government has continued to push its false and distorted narrative aggressively in an apparent attempt to inflame Korean public opinion, manipulate U.S. policymakers, and provide cover for its whole-of-government effort to eliminate Coupang as a competitor to the Government's favored Korean and Chinese companies.

The objective facts are as follows. On November 18, 2025, Coupang discovered a limited data breach related to customer accounts. The company immediately began an internal investigation and retained leading cybersecurity firms, including Google's Mandiant, Inc., and Palo Alto Networks. The cybersecurity firms determined that the breach had been perpetrated by a Chinese former employee based in China (the "Threat Actor"), who relied on insider knowledge and a restricted "fallback key" from his time working at Coupang to forge authentication tokens and access the customer data.

The Threat Actor gained access to approximately 33 million Coupang customer accounts. Fortunately, the Threat Actor downloaded and retained data from only approximately 3,000 accounts. The information that the Threat Actor accessed was limited to names, email addresses, phone numbers, shipping addresses, certain order histories, and building codes to shared spaces where packages could be delivered, and did not include any financial information such as credit card data, Government-issued identification numbers, login credentials, or home entry codes. There is currently no evidence that any of the stolen data was sold, transferred, or shared. The Threat Actor never made any blackmail or similar threats and has repeatedly stated that the data never left his control.

Coupang promptly disclosed the data breach to the Government and began working closely with Government agencies, especially the National Intelligence Service (the "NIS"), to ensure the breach was contained. Coupang's investigation into the breach was done at the express direction of the NIS over a period of several weeks, during which time Coupang and the NIS closely coordinated their efforts.

At the NIS's direction, Coupang secured the Threat Actor's cooperation with their containment efforts, met with the Threat Actor in China, and recovered the devices he used in connection with the breach. The NIS provided Coupang with guidance on issues like how to

approach the Threat Actor and recover the devices. Despite the substantial risks inherent in such an operation, Coupang did what the NIS asked, in an effort to eradicate any remaining threat to its customers.

During this time, the NIS requested that Coupang keep the operation confidential, which Coupang did, all while the Government continued to falsely accuse Coupang of failing to seriously address the breach.

In addition to its cooperation with the Government, Coupang also quickly took steps to address customer and public concerns about the breach. On November 29, 2025, Coupang publicly disclosed the breach in Korea and the United States through a press release and filed an 8-K with the U.S. Securities and Exchange Commission on December 15, 2025. Later in December 2025, Coupang reported the results of its joint investigation with the NIS to Government authorities and provided an update to potentially affected customers.

D. The Government Uses the Threat Actor's Data Breach as a Pretext to Launch a False and Defamatory Public Relations Campaign Against Coupang

Almost immediately after Coupang publicly disclosed the breach, the Government began misrepresenting the facts in the press to create a smokescreen for the massive administrative assault on Coupang it was about to launch.

The Government made myriad false statements about the breach, starting on December 1, 2025, the first day that Coupang stock traded on the NYSE following the disclosure. A senior official in President Lee's office asked whether Coupang took the breach lightly because it operates in Korea and suggested that the company would have been forced to shut down if it operated in the United States because of punitive damages.

The idea that any legal case brought against Coupang in the United States based on a data breach affecting only 3,000 customer accounts with no claims of financial harm could succeed, much less that punitive damages could be recovered, is speculative; the notion that a multinational corporation with a market capitalization of tens of billions of dollars would have to shut down because of any such punitive damages is ridiculous.

The statement portrayed the breach as far worse than it actually was, and painted Coupang as an irresponsible U.S. company harming Koreans. President Lee and his allies would continue to develop these themes in the coming weeks.

The next day, December 2, 2025, President Lee publicly stated that "strict accountability must be enforced" against Coupang and called for "relevant ministries" to increase fines against Coupang and make punitive damages available. President Lee also stated that companies violating data security rules should be hit with fines "so severe that they go out of business," and, in a clear reference to Coupang, asked, "Aren't there some 34 million victims?"

On December 3, 2025, during a National Policy Committee session, Chairman Yoon Han-hong stated, “It is no exaggeration to say that, essentially, the personal data of all South Koreans except those under 14 years old have been leaked.” But this does appear to have been an exaggeration—and a massive one, by more than four orders of magnitude. Yoon claimed that the data of every adult Korean had been breached, when in fact, the available evidence shows that it was the data of only 3,000 accounts. At the same session, another committee member expressed hope that the committee would refer Coupang Inc. Chairman Bom Kim (“Kim”), a U.S. national, for prosecution.

Even though there was no evidence that any of the customers affected by the data breach were financially harmed, and the breach seemed to have been fully contained, within days of the breach being disclosed, President Lee and others in the Government still threatened Coupang’s existence and the company’s Chairman.

About a week later, on December 10, 2025, Park Dae-joon, the Representative Director of Coupang Corp., resigned from his position under Government pressure, stating that he was “very sorry that we disappointed the public with the recent personal data incident,” and that he “share[d] the grave responsibility regarding the occurrence of the leakage and how it was handled.” In the wake of Park’s resignation, Harold Rogers, the Chief Administrative Officer and General Counsel of Coupang Inc., and a U.S. national, was appointed as the interim Representative Director of Coupang Corp.

Also on December 10, 2025, when the limited scope of the breach and the lack of harm were even clearer, President Lee again called for significant penalties to be imposed against Coupang. The following day, December 11, 2025, while referring to the breach, President Lee advocated for the creation of a class action system in Korea, so that “when [companies] harm the public, penalties [are] strong enough to make companies fear they could collapse.” That is, President Lee implied that the breach at Coupang was so serious it required a material change to Korea’s legal system. President Lee further discussed the need to increase financial sanctions, singling out Coupang and suggesting that its executives were not sufficiently afraid of punishment.

On December 11, 2025, President Lee also began attacking Coupang in public outside the context of the data breach, alleging that special regulations were necessary for Coupang because of how badly they overworked their employees. “There’s a 50% premium for work between 10 p.m. and 6 a.m., but this is too harsh. Isn’t it because of night work that so many die? Some argue we should ban this…. Coupang’s employment structure…seems like a new form of labor requiring new regulatory approaches.”

The next day, December 12, 2025, President Lee again suggested that the breach at Coupang was so severe that Korean law should be changed, in this case to permit higher fines. Current law allows for a fine of up to 3% of a company’s average revenue over the preceding three years. It has been reported that, for Coupang, this could mean a fine of over $800 million, which would be the largest fine imposed against a company in Korean history.

President Lee seems to believe that, at least for a U.S. company, even a historic fine would be too small for a data breach affecting only 3,000 customer accounts with no indication of financial harm. The Government has never previously recommended imposing a fine that approaches the 3% limit against any company—but some DPK lawmakers have recently suggested that the limit should be increased from 3% to an astounding 10% of revenue, and applied retroactively to Coupang.

On December 17, 2025, the Government's public relations campaign against Coupang escalated further when the National Assembly Science, ICT, Broadcasting and Communications Committee (the "SIBCC") held a hearing focused on the data breach. One Representative from the DPK, President Lee's anti-U.S., pro-China party, called for interim Representative Director Rogers to be "kicked out of South Korea." Another called for Coupang to "go out of business." Yet another threatened Coupang's existence with chilling language: "The sandcastles that Coupang built can crumble overnight. Keep in mind that today's hearing is the beginning of the end."

On December 19, 2025, President Lee's Prime Minister Kim Min-seok urged Government regulators to approach enforcement against Coupang for the data breach "with the same determination used to wipe out mafias." Prime Minister Kim added that regulators should "not worry about staffing, and impose strong economic sanctions" on Coupang—"market order" would be restored, and this was "not a time for academic correctness, but for decisive and bold action." By "academic correctness," Prime Minister Kim seems to have been referring to the rule of law.

On December 25, 2025, Coupang issued an accurate press release describing its investigative findings, stating that the Threat Actor had "accessed 33 million accounts, but only retained user data from approximately 3,000 accounts," "subsequently deleted the user data," and "never transferred any of the data to others." Coupang further correctly stated that the data the Threat Actor stole "was only ever stored on his personal desktop PC and MacBook Air laptop," "[a]ll devices and hard drives the perpetrator used to leak Coupang user data have been retrieved and secured following verified procedures," and "Coupang has also been cooperating fully with all relevant ongoing government investigations."

On December 26, 2025, despite all the evidence to the contrary, the NIS publicly and falsely denied directing Coupang to make contact with the Threat Actor and retrieve the devices with the stolen data from China.

On December 28, 2025, in the face of this relentless campaign from the Government, Coupang Inc. Chairman Kim apologized for the data breach, stating that he could not "express how deeply disheartened" he was "by the current situation that has disappointed so many people." On December 29, 2025, Coupang announced a compensation plan for affected customers. Pursuant to the plan, Coupang offered vouchers worth over $34 (50,000 won) to each of the 33 million customers whose data could have been—but was not in fact—compromised by the Threat Actor. The vouchers could be used on Coupang products, Coupang food delivery, Coupang travel, and Coupang luxury beauty shopping. In total, the value of the vouchers was over $1 billion.

On December 30, 2025, in apparent recognition that the Government's actions toward Coupang could be illegal, a DPK lawmaker stated, "U.S. authorities, such as the U.S. Trade Representative, have not issued any official messages on Coupang, so Korea does not have to care much for any possible trade risk with the U.S. due to the latest incident."

The same day, Rogers began the first of two days of testimony at a National Assembly hearing. Among other topics, Rogers testified that Coupang's investigation into the data breach was conducted at the direction of the NIS. As discussed above, this was true. At the hearing, numerous DPK Representatives called for travel bans to be imposed against Coupang executives, and for customers to abandon the company.

Following Rogers' testimony, DPK Representative Seo Young-kyo called for "severe sanction[s]," and as many other Government officials had already done, significantly overstated the scope of the breach. The NIS also issued a statement claiming that Rogers' statements about Coupang's investigation being conducted at the behest of the NIS were "entirely untrue," and called for him to be criminally indicted for perjury. The National Assembly would soon answer this call.

On December 31, 2025, Rogers gave the second day of his testimony at the National Assembly hearing. The statements from DPK lawmakers during the second day of the hearing were even more inflammatory. KFTC Chairman Ju Biung-ghi threatened that "we can consider penalties up to and including a suspension of business operations" of Coupang, which could devastate the company. Ju also discussed the possibility of ordering Coupang to divest its affiliates.

Representative Jung Hye-kyung also pressured the Director of the National Pension Service—which at the time held approximately $150 million of Coupang shares—to fully divest its Coupang holdings and exclude the company from future portfolio allocations, all of which may have caused Coupang's share price to decline.

Multiple DPK Representatives advocated for the criminal prosecution of Coupang executives. One DPK lawmaker stated, "We must seize this opportunity to block criminal groups like Coupang from operating in our society." Another suggested that, "If necessary, we should even cooperate with Interpol to bring" Coupang Inc. Chairman Kim, a U.S. national, "to the Korean court." They also repeated their calls for travel bans to be imposed against Coupang executives, and threatened to criminally refer Kim for tax evasion. Of course, there does not appear to have been any evidence that Kim committed tax fraud, and the data breach had nothing to do with tax. What is more, the Government had already investigated Coupang for tax evasion in 2024, based on its connections to the U.S., and never announced any finding of wrongdoing.

On December 31, 2025, in response to the NIS's request, the National Assembly voted to refer U.S. national Rogers for a criminal perjury investigation, based on his truthful testimony regarding the NIS's direction of Coupang's investigation of the data breach. Former Coupang Corp. CEO Park Dae-joon and two other Coupang Corp. executives were also criminally referred. The National Assembly further voted to refer for criminal prosecution U.S. national

Kim, Coupang Inc. Vice President Kim Yoo-seok, and former Coupang Corp. CEO Kang Han-seung for failing to appear at the hearing. This point bears emphasizing—because he did not show up at a hearing, the Government threatened to indict the U.S. national Chairman of a Fortune 150 company listed on the NYSE.

The same day, Kim Younghoon, President Lee's Minister of Employment and Labor, announced that he had instructed officials at his agency that "if they contact public officials who transferred to Coupang, they should know they will ruin their careers."

On January 5, 2026, a DPK Representative held a press conference to condemn Coupang as "an illegal, anti-labor, anti-social, anti-human rights, criminal enterprise," asserting that it was destroying small businesses and the "foundation of the local economy."

On January 8, 2026, the Institute of National Security Strategy, an organization funded by the NIS, published a report describing the data breach as a "national security issue" and a "digital security air-raid alert" that was "capable of leading to the collapse of the national economic system."

On January 13, 2026, following reports that Rogers had left Korea, the Seoul Metropolitan Police Agency (the "SMPA") "requested the Ministry of Justice to notify them upon Rogers' entry into Korea and plan to impose a travel ban if he returns," which would prevent Rogers from leaving Korea. As noted, Rogers is a U.S. national and an executive of a U.S. Fortune 150 company, and is not a Korean national.

On January 16, 2026, Kim Yongbeom, President Lee's Chief of Staff for Policy, gave an interview in which he said that "Coupang is operating too illegally, and continuing this way is problematic. Coupang has an overwhelming influence on our national economy and purchasing, yet it doesn't fully fall under our jurisdiction (because it's a U.S. company), which is quite a significant problem."

Also on January 16, 2026, speaking from Washington, D.C., where he had been sent by President Lee to address concerns that U.S. officials had raised about the Government's draconian response to the data breach at Coupang, South Korea's top trade envoy Yeo Han-koo dismissed accusations that the Government was discriminating against the company. Yeo stated that "[t]he fact of the matter is that there was a data-breach incident" at Coupang "that, in terms of scale, is unprecedented in Korean history. About 33.7 million people's very private information was breached, amounting to almost 80 percent of Korea's adult population."

This statement was false. As discussed above, the data of 3,000 people, not 33 million, was breached. This had been established for weeks before Yeo's statement. Nor was the breach the largest in Korean history, or even close to it. As described below, some of Coupang's Korean and Chinese competitors have experienced far worse breaches, involving far more sensitive information, although the Government's response to those breaches was muted.

Yeo further claimed that the breach encompassed "apartment entrance passkey passwords. So this is directly related to the safety and privacy of every individual citizen." This

statement was also false—the Threat Actor downloaded 2,609 building codes to shared spaces where packages could be delivered, not 33 million apartment entrance passkeys. Coupang does not even collect apartment entrance passkeys from its customers. Yeo thus inflated not only the scale of the breach, but also its nature, creating the false impression that the Threat Actor and anyone to whom he had given the stolen data could have physically entered Coupang customers' homes.

As recently as yesterday, weeks after the relevant facts of the data breach became widely known, the Government has continued its broad dissemination of false information, which seems designed to distract Korean and U.S. audiences from the true intent behind the Government's assault on Coupang. On January 21, 2026, President Lee's Chairman of the PIPC, Song Kyung Hee, claimed it was "certain" that "the personal information of more than 30 million Coupang members was leaked, and if we add nonmember information (such as delivery addresses and phone numbers of nonmembers like family members entered by subscribers), the scale is likely to grow further." It is not "certain" that the data of 30 million Coupang customers was leaked; to the contrary, all the available evidence appears to establish that data related to only 3,000 Coupang accounts was breached. Projecting assurance, Song, like other DPK officials before him, thus alleged that the breach was about 10,000 times larger than it actually seems to have been.

The Government did not limit its public relations campaign to disseminating false information—it also tried to suppress countervailing information that was true. On January 14, 2026, the Personal Information Protection Commission (the "PIPC") ordered Coupang "to take down its independent probe results" that it had published on December 25, 2025, "describing them as unverified information," and stating that the company's press release "could be considered as interfering" in the PIPC's investigation. The PIPC also "noted Coupang has been uncooperative with its investigation by delaying or failing to submit requested documents," and warned that "such acts could be considered in possible future penalties." The PIPC further suggested that Coupang had presented the findings in its release "as if authorities had verified them," and that the release could "mislead users and undermine an ongoing official investigation."

To recapitulate, a Chinese former employee of Coupang based in China illegally used confidential information to download data from 3,000 Coupang customer accounts, which did not include the most sensitive categories of data. Coupang reported the breach to the Government, and cooperated with the Government to recover the data and contain the breach. No customers have reported any financial losses.

In response, the Government threatened to bankrupt Coupang, suspend its business license, and impose the largest fine in Korean history against it; referred for criminal prosecution, and imposed travel bans against multiple Coupang executives, including U.S. nationals; described Coupang as a criminal and illegal organization and compared it to the mafia; repeatedly mischaracterized the scope and type of the data breach, making it sound much worse than it actually was; pressured Korean pension fund managers to sell Coupang stock; and tried to prevent Coupang from telling the truth about the breach to the Korean public.

Unfortunately, the Government's actions have been just as discriminatory and disproportionate as its rhetoric.

E. The Government Uses the Threat Actor's Breach as a Pretext to Launch an Administrative Assault on Coupang

Shortly after Coupang's public disclosure of the data breach, the Government launched an administrative assault on the company that is breathtaking in its range, speed, and intensity. It bears no relation whatsoever to the limited nature of the breach, and involves almost every agency under the Government's control, including many agencies that have no jurisdiction over matters involving data, cybersecurity, or privacy. Hundreds of Government officials from those agencies have been pressed into service as shock troops. Contrary to the Government's claims, it is the Government's assault on Coupang, not the data breach, that is truly unprecedented.

A complete accounting of all the Government's illegal actions exceeds the scope of this letter. If it becomes necessary for the U.S. Investors to file claims against Korea, they will bring the full ledger to the arbitration. But the following examples should give some sense of how arbitrary and capricious the onslaught has been.

On December 8, 2025, nine days after Coupang publicly disclosed the data breach, the KFTC began investigating whether Coupang's membership cancellation process for certain of its services violates the Electronic Commerce Act (the "ECA") as a "dark" or deceptive practice. The KFTC informed Coupang that it was required to propose ways to change its cancellation process—before the KFTC had even determined that the company violated the ECA. The KFTC is also closely reviewing the terms and conditions that govern all of Coupang's services for other possible violations. On December 10, 2025, the KFTC conducted on-site work at Coupang's corporate headquarters in Seoul in furtherance of these investigations.

There is no indication that Coupang's membership cancellation process or its terms and conditions are in fact illegal. The more important point is that, given the Government's public statements and the timing, it appears that the KFTC, an economic competition agency, began its investigation because of the data breach, not because of anything to do with antitrust. Using the powers of a disparate agency to punish a company for an unrelated infraction is quintessentially arbitrary behavior from an authoritarian regime, and a recognized indicator of creeping expropriation. Similar conduct appears throughout arbitration awards against countries like Venezuela and Russia.

The next day, December 9, 2025, the SMPA's Cyber Investigation Division raided Coupang's corporate headquarters in Seoul.

On December 18, 2025, the Government announced the creation of an inter-ministerial task force focused on the data breach. The agencies involved include the National Police Agency; the PIPC; the Financial Services Commission, a financial regulator that chiefly supervises banks and would not typically participate in an investigation involving neither financial information nor financial institutions; the Korea Media and Communications Commission, which, as its name implies, regulates media companies, not retail ones; and the

NIS, whose primary role in the pertinent events was to direct Coupang to take actions that it could not take itself for fear of diplomatic friction with China. The task force was later expanded and became even larger.

There have been many other data breaches in Korea, some of them far more serious than the incident at Coupang, but the Government does not appear to have previously formed an inter-ministerial task force of this kind to investigate a private-sector breach. Indeed, this marks the first time that a Korean national intelligence agency has intervened in a security incident at a private company.

On December 22, 2025, the NTS created its own 150-member task force, focused solely on Coupang. The task force is led by a division of the NTS colloquially referred to in Korea as the "grim reaper" of the finance industry, based on its supposed similarities to the historical Central Investigation Department, which was known for carrying out investigations as a form of political retaliation. By way of comparison, just last year, the NTS created special task forces to uncover high-value tax delinquencies, related to nearly $75 billion in unpaid taxes. Those task forces totaled only 56 members.

As these sorts of investigations, raids, and inspections began to proliferate, Coupang had no choice but to expend tremendous resources responding to each of them, draining the company of time, energy, and money that would have been much better spent running its business and serving its Korean customers. Approximately 400 Government investigators have been deployed against the company. They have already conducted at least 150 face-to-face meetings and 200 interviews and made over 1,100 document and other information requests. The sheer number of Government officials stationed at Coupang's headquarters and their continuous demands have been paralyzing. Coupang employees have complained that "there are no remaining conference rooms," they have been "creating various materials" for the Government "for over a month," and they "can't work" because they are "responding to face-to-face interview requests."

This total disruption seems to be the Government's point. There is no plausible purpose for this Orwellian exercise other than to obstruct Coupang's operations so fundamentally that it can no longer compete effectively with Naver and its other Korean and Chinese competitors.

On December 25, 2025, President Lee convened an emergency meeting, where the participants discussed "other punitive sanctions including large-scale fines" against Coupang, along with "comprehensive pressure measures including not only fines but also revoking delivery business service licenses and conducting intensive tax audits." President Lee invited "officials from the diplomatic and security sectors" to the meeting "to discuss the possibility of the Coupang incident escalating into a diplomatic conflict between South Korea and the United States." If the Government's assault on Coupang is not pretextual, and is actually about the data breach, as President Lee and his allies have claimed, then it is difficult to understand why they believe it could cause a diplomatic conflict between the United States and Korea.

On December 29, 2025, the Ministry of Science and ICT and the PIPC "amended the eligibility criteria for Korea's Information Security Management System-Personal (ISMS-P),

inserting new grounds for revocation." If Coupang's ISMS-P certification were revoked, the company could be subject to substantially larger fines, thereby undermining its ability to run its business. Ex post facto laws and regulations—it is as though the Government is following an expropriation playbook.

The same day, the Korea Customs Service launched an on-site investigation of Coupang's Seoul headquarters related to foreign exchange transactions at Coupang's U.S. headquarters. By definition, this customs investigation was unrelated to the data breach.

On January 2, 2026, the SMPA—itself already part of a six-ministry task force focused on the data breach—formed a task force of its own centered on Coupang. The SMPA had previously formed its own task force to focus on the breach. In the recent past, the SMPA has formed special task forces to address critical national issues like stock price manipulation (37-50 members); widespread kidnapping, detention, and torture by criminal organizations operating in Cambodia (44 members); and cryptocurrency fraud involving millions of dollars (30 members). The number of officers assigned to the Coupang task force is 86.

On January 5, 2026, Lee Chanjin, President Lee's Governor of the FSS, "warned of a rigorous investigation" into Coupang's interest rates on merchant loans, accusing Coupang of "excessive profit" and "bullying," even though its rates are within legal limits. The relationship between the data breach and merchant loan interest rates is not obvious.

For many months, Coupang has been planning to form a real estate investment trust (the "REIT") and raise money to securitize its logistics centers. On January 6, 2026, the Ministry of Land, Infrastructure and Transport ("MOLIT") withheld approval for the plan. Acknowledging the unusual nature of MOLIT's obstruction, the Director of the Investment Policy Division stated, "We are reviewing the matter in detail without regard to the usual time required for business approvals." How the securitization of Coupang's logistics centers relates to the data breach is similarly unclear.

Relatedly, a DPK lawmaker sent an official document to certain financial institutions about their potential investment in the REIT, alleging to these future Coupang partners that the company's practices violate ESG management principles and requesting information as to whether the institutions have any plans to participate in asset liquidations intended to increase the personal wealth of Kim.

On January 6, 2026, the Government apparently concluded that it still did not have enough task forces focused on Coupang, and created another one, this time at MOEL, to investigate the company using "all possible means." It promised that any violations would "be met with strict measures."

On January 13, 2026, the KFTC's Enterprise Group Bureau, Market Surveillance Bureau, and Distribution Agency Bureau dispatched 20 investigators to Coupang's corporate headquarters in Seoul to collect materials apparently unrelated to the data breach. By the next day, the KFTC was planning an "unprecedented" two-week on-site investigation of Coupang,

deploying a large number of investigators, which also seemed to be disconnected from the breach.

On January 14, 2026, MOLIT requested that local governments conduct inspections of all 387 of Coupang's facilities throughout the country. MOLIT is tasked with supervising national territory, water resources, road and housing construction, and land reclamation—data breaches are not part of its ambit.

On January 16, 2026, MOEL announced that it would deploy 17 labor inspectors to conduct "an intensive investigation into allegations including illegal dispatch, the creation and management of a blacklist, and operation of a low-performer exit program" at Coupang. The investigation did not pertain to the data breach.

In sum, over the past six weeks or so, in response to a limited data breach involving only 3,000 customer accounts, the Government has marshalled against Coupang the resources of at least 14 different agencies, and 4 separate task forces and teams; undertaken scores of investigations, inspections, and raids of the company, most of which have nothing to do with the breach; and mobilized hundreds of Government officials in service of these efforts.

Even if the Government's public statements disparaging Coupang were disregarded, these actions would speak for themselves. It is impossible to reconcile them with the objective facts of the data breach. They demonstrate that the Government is severely discriminating against Coupang because it is a successful U.S. company that threatens the traditional dominance of the Government's preferred Korean and Chinese competitors.

These are not the actions of a Government that respects the Treaty, international law, or the time-honored partnership between Korea and the United States.

F. The Government's Response to More Severe Data Breaches by Korean and Chinese Competitors Further Proves its Discrimination Against Coupang

Lastly, a comparison of certain other data breaches that occurred at Korean and Chinese companies, and were significantly more damaging than the breach at Coupang, is instructive. The Government's response to those breaches, or lack thereof, provides further proof of how punitive, disproportionate, and discriminatory the Government's response to the breach at Coupang has been.

An illustrative breach occurred recently at Kakao Pay, a Korean mobile payments service provider. Kakao Pay's parent Kakao is a Korean competitor of Coupang. In 2024, it emerged that, over the preceding six years, Kakao Pay had intentionally transferred 54 billion personal data records of 40 million Korean customers to Alipay Singapore, including sensitive financial information such as account balances, transaction histories, and credit information. Alipay is owned by Ant Group, a Chinese affiliate of the Chinese conglomerate Alibaba Group Holding Limited ("Alibaba").

Kakao Pay's conduct was vastly more serious and damaging than that of Coupang. At Kakao Pay, it was not a rogue former employee who effected the breach, in violation of the company's policies and procedures—it was the company itself that deliberately caused the breach, to generate revenues by sending the data to a Chinese conglomerate's subsidiary in a foreign country. Yet rather than threaten Kakao Pay with annihilation, or form multi-agency task forces to investigate every facet of its business, the Government imposed small fines of $15 million, and the company's CEO received a "formal warning" that led to neither his dismissal nor his prosecution.

Another example that underscores the discriminatory treatment Coupang faces as a U.S. company involves SK Telecom ("SKT"), Korea's largest wireless carrier. In April 2025, SKT experienced a massive cyberattack involving SIM card data from 23–27 million customers—the company's entire user base. This represents a breach of the data of more than 7,000 times the number of customers whose data was downloaded in the Coupang incident. And yet, the Government imposed a fine against SKT of $91 million, more than eight times smaller than the fine President Lee has threatened to impose against Coupang. Nor does SKT appear to have faced a whole-of-government effort to disrupt its business, criminal referrals of its executives, or calls from leading politicians for its collapse and bankruptcy.

The even more recent Upbit data breach from November 2025 also provides a stark contrast to the Coupang situation. Upbit is Korea's largest cryptocurrency exchange. In September 2025, Naver announced that it would acquire the company. In a cyberattack attributed to North Korea's Lazarus Group, hackers penetrated Upbit to steal over $30 million of customer cryptocurrency assets, during which they may have also exposed user data. The SMPA began a probe, the FSS issued warnings for "serious" security failures, the Government began an investigation for possible reporting delays, and the National Assembly considered legislation to strengthen the regulation of crypto exchanges—but the Government response ended there.

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

These examples are merely illustrative, not exhaustive. And as discussed above, this pattern of harsh punishment for Coupang, but minor reprimands for Korean and Chinese companies that engage in much worse conduct, holds true outside the data breach context. Based on this evidence, it is apparent that the Government illegally applies one standard to U.S. companies, and another to the Korean and Chinese companies with which they compete.

II. Treaty Violations

Through the measures described in this letter, and related conduct, the Government has violated Korea's obligations under the Treaty, including without limitation the obligation to

accord covered investments fair and equitable treatment and full protection and security (Article 11.5); to accord treatment no less favorable than that accorded to investors and investments of Korea and third countries (Articles 11.3 and 11.4); the prohibition on direct or indirect expropriation without prompt, adequate, and effective compensation (Article 11.6); and the obligation to observe commitments entered into with respect to covered investments (Article 11.5(2)).

For purposes of this letter, the Claimants are Mr. Neil Mehta and Mr. Benjamin Peretz, who are U.S. nationals. Their principal business address is 4 Orinda Way, Orinda, California 94563, United States of America. Their ownership rights and interests in Coupang are covered investments under the Treaty. This letter serves as the notice required by Article 11.16.2 of the Treaty regarding the Claimants' intent to file arbitration claims against Korea. There are additional U.S. Greenoaks and Altimeter entities who have ownership rights and interests in Coupang and who qualify as investors under the Treaty. Their principal business addresses are 4 Orinda Way, Orinda, California 94563, United States of America, and One International Place, Suite 4610, Boston, Massachusetts 02110, United States of America, respectively.

The Claimants reserve the right to assert additional breaches of the Treaty, and to seek compensation for the losses and damages they have suffered, and continue to suffer, as a result of Korea's continuing and escalating violations of the Treaty and international law.

Damages will be specified at a later stage, but the Claimants currently estimate their losses to be no less than hundreds of millions of dollars. Overall, the losses of all investors in the United States are no less than tens of billions of dollars.

III. Conclusion

This notice is submitted with due regard for Korea's longstanding status as a close ally of the United States and a reliable destination for billions of dollars of U.S. investment. The Government's unlawful conduct toward Coupang, however, raises serious concerns about Korea's continued respect for the rule of law—concerns that are increasingly shared by other U.S. investors and U.S. policymakers.

For their part, lawmakers, businesses, and members of the public in Korea recognize the risk to the country's future that a shift away from a rules-based investment framework, toward a new approach governed by political whims and shifting international alliances, would pose.

The Government's illegal actions toward Coupang have already had material economic consequences. The company's share price has declined; equity analysts have issued downgrades; U.S. class actions and related proceedings have multiplied; and Naver, Coupang's principal domestic competitor, has taken advantage of the company's situation. The Government's actions have deeply distressed U.S. investors—those who currently own the stock of Coupang, other U.S. companies operating in Korea, and Korean companies alike.

The U.S. Investors do not seek arbitration lightly. Their primary goal is corrective action, including the cessation of the discriminatory, disproportionate, and arbitrary measures described

in this letter and the establishment of a stable environment in which Coupang can successfully run its business, free from political targeting and interference.

Korea faces a clear choice: allow an egregious abuse of state power to continue, or reaffirm its standing as a country where U.S. companies can operate with confidence and U.S. investors can deploy capital with conviction.

As contemplated by the Treaty, the U.S. Investors invite the Government to engage in good-faith consultation to resolve this dispute amicably. But if the situation with Coupang is not promptly resolved, the U.S. Investors will be compelled to pursue arbitration to protect their investments in the company and vindicate the rule of law.

Sincerely,

Marney L. Cheek
David Z. Pinsky
Clovis Trevino
Counsel for the U.S. Investors

cc: Ambassador Kang Kyung-wha
Embassy of the Republic of Korea in the United States of America
2450 Massachusetts Avenue N.W. Washington, D.C. 20008
United States of America