Coupang Data Breach Crisis Analysis

December 30, 2025

Contents

Executive Summary

1. The Incident: Scope & Management Failure

- **Scale of Breach:** In late November 2025, Coupang confirmed the largest data leak in South Korean history, affecting **33.7 million accounts** (approx. two-thirds of the population).
- **Root Cause:** The breach was not a sophisticated external hack but an **insider-driven failure**. A former employee utilized an unrevoked security key to access records.
- **Data Exposed:** Personal identifiers (names, addresses, phone numbers) and order history. **Critically, no payment details (credit cards) or passwords were compromised.**
- **Management Response:** The response was criticized as opaque and delayed. Founder Kim Bom did not apologize until late December, causing a public outcry. CEO Park Dae-jun resigned; Harold Rogers was appointed interim CEO.

2. Operational Risk & Regulatory Outlook

- **Suspension Threat:** While the KFTC (Korea Fair Trade Commission) has threatened a business suspension, analysis suggests this is a **low-probability leverage tactic.**
- **Regulatory Reality:** Precedents (e.g., SK Telecom, Nexon) indicate regulators prioritize consumer stability. A suspension would disproportionately harm millions of consumers and SME merchants.
- **Likely Outcome:** strict corrective orders and significant, albeit affordable, monetary penalties, but expects **operations to continue** without interruption.

3. Financial Impact & Stress Test

- **Estimated Cost:** The total financial impact is estimated at **$2.0B – $2.5B (~2x current FCF)**.
    - **Compensation:** ₩1.685 trillion (~$1.17B) in customer vouchers (non-cash expense).
    - **Fines & Remediation:** Est. $500M–$800M in fines plus IT security upgrades.
- **Liquidity Assessment:** Coupang is well-positioned to absorb this shock. The company holds **$7.3B in cash** and generates ~$1.2B in annual Free Cash Flow. While the breach may wipe out 1–2 years of profitability, it **does not threaten solvency or liquidity.**

4. Investment Thesis & Valuation Impact

- **Structural Moat Intact:** Despite the reputational hit, the "Rocket WOW" ecosystem lock-in remains resilient. Early data shows only a single-digit decline in Daily Active Users (DAUs) rather than a mass exodus. The convenience and logistics dominance of Coupang continue to outweigh privacy concerns for the majority of users.
- **Valuation Analysis:** The stock has corrected **~25%** due to sentiment and uncertainty.

- **Intrinsic Value:** Adjusting for the one-time financial hit and increased governance risk premium, the report estimates the intrinsic value decreases by only **~5%**, suggesting a disconnect between the current price drop and the fundamental long-term value.

1. Incident Breakdown & Forensics

Full Timeline

Coupang's data breach unfolded over several weeks in late 2025. On 18 November 2025, the company's security team detected unusual access activity, initially affecting only around 4,500 user accounts. Coupang quietly notified regulators on 20 Nov with this preliminary figure, seemingly hoping the incident was contained. However, further investigation revealed the problem was far more extensive. On 29 November 2025, Coupang publicly admitted that a staggering 33.7 million customer accounts had been compromised. This update meant nearly two-thirds of South Korea's population were impacted, making it the largest data leak in Korean history. The breach exposed personal information including customers' names, phone numbers, email and physical addresses, and purchase histories. (Fortunately, no payment details or passwords were taken, according to company and regulatory reports.) Coupang alerted affected users via text message on 29–30 Nov when disclosing the full scale. In early December, the government launched a pan-agency investigation, even raiding Coupang's headquarters as evidence-gathering began. By late December, as political pressure mounted, Coupang's founder issued a formal apology and the company announced a compensation plan (details below). In summary, what initially looked like a minor incident in mid-November snowballed into an unprecedented breach of 33+ million accounts by month's end, drawing intense public and government attention.

Nature of the Breach

Investigations revealed that the breach was not a sophisticated external hack, but an insider-driven lapse. A former Coupang employee was identified as the culprit: he had stolen an internal digital security key prior to his departure and later used it to access the company's core user database. Exploiting this undisabled credential, the ex-employee illicitly accessed around 33 million customer records on Coupang's servers. This points to a serious access control failure: Coupang did not adequately revoke or change critical access keys when the staff member left, allowing a backdoor into the system. According to Coupang's forensic findings, the perpetrator saved data for roughly 3,000 accounts onto personal devices (a desktop and laptop) before being caught. Those devices (including a laptop the suspect tried to dump in a river) were later recovered by the company and police, and the individual confessed. The stolen data itself consisted of "basic" personal info (names, phone numbers, emails, addresses, and some order details) and did not include highly sensitive data like login passwords, payment card numbers or financial info. There were 2,600 cases where delivery instructions (like building entrance codes) were exposed, which is a privacy concern but not financial fraud risk. Importantly, investigators have not found evidence of the data being sold or leaked to third parties; it appears the ex-employee acted alone and the data copies have been contained. From a technical perspective, the breach highlights encryption and monitoring weaknesses: an internal key provided broad access to unencrypted customer records, and the abnormal data queries went unnoticed for months. (Korean police indicated the breach went undetected for about 5 months before November.) In summary, Coupang suffered a systemic internal security breakdown: insufficient off-boarding security (allowing an ex-staffer to retain a key), lack of

robust encryption/isolation for customer data, and delayed intrusion detection, all of which combined to enable one rogue insider to compromise millions of records.

Management Response

Coupang's handling of the breach has been widely criticized as slow and opaque, falling short of industry best practice. The company's initial instinct was to downplay the incident, when first reporting it, Coupang used the term "data exposure" rather than "leak" and suggested only a few thousand users were affected. It then went mostly silent for over a week even as internal evidence mounted that tens of millions of accounts were compromised. The founder and CEO, Kim Bom, did not make any public statement until almost five weeks after the breach was discovered. It was only on 28 December 2025 that Kim issued a public apology, long after regulators and the public had been clamoring for answers. In his statement (posted in Korean on Coupang's site), he acknowledged the company's failure to communicate promptly and called his decision to wait for "100% of the facts" before speaking a "wrong judgment". Kim admitted that Coupang's silence had fueled customers' fear and anxiety, and he took personal responsibility, expressing "sincere apologies". By the time of this apology, public anger was intense. In mid-December, Coupang had sent only its newly appointed interim CEO and other executives to a National Assembly hearing, while Kim Bom (a U.S. citizen) remained abroad, citing "other appointments". Lawmakers berated his absence as "insulting the public" and accused him of hiding behind his foreign citizenship. This perception – that management was evasive and unaccountable – sparked protests and calls for boycott. Consumer groups even staged rallies in Seoul urging people to quit Coupang over the company's dismissive attitude.

In terms of concrete responses, Coupang did take several steps: it brought in outside cyber security firms (Mandiant, Palo Alto Networks, EY) to investigate and assist; it cooperated with police and government agencies (albeit belatedly, after an initial attempt to investigate internally); and notably, it forced leadership changes. Park Dae-jun, Coupang's Korea CEO, resigned on 10 December to take responsibility for the incident. He was replaced by Harold Rogers (previously Coupang's Chief Administrative Officer in the US) as interim CEO for Korea. Rogers attended the parliamentary hearing on 17 Dec, but his vague and legalistic answers (alongside Coupang's Chief Security Officer) only heightened frustration. The overall consensus is that Coupang's management response lagged industry standards. Best practice for breaches calls for timely disclosure, CEO visibility, and frequent updates to maintain trust. Coupang instead went quiet, then was perceived as minimizing the issue and avoiding accountability. By comparison, when Korea's SK Telecom suffered a large data breach earlier in 2025, its CEO promptly apologized and the company swiftly announced compensation measures. Coupang's delayed response allowed anger to fester. The company has since been scrambling to repair the damage, Kim Bom-suk's late apology and a ₩1.68 trillion (~$1.2 billion) compensation plan are attempts to restore goodwill (discussed later). But reputationally, management's credibility has been dented. Polls showed 69% of respondents believed Chairman Kim was "avoiding accountability" by staying abroad. Going forward, we (and other investors) will be watching whether Coupang's leadership can learn from this fiasco, strengthening its crisis response playbook, or whether deeper governance issues persist.

2. Operational Risk & Regulatory Deep Dive

Business Suspension Threat

In the wake of the breach, Korean regulators, notably the KFTC (Korea Fair Trade Commission), raised the specter of an unprecedented penalty: suspending Coupang's operations. On 18 December, the Minister of Science and ICT told a National Assembly hearing that his ministry

was consulting with the KFTC, which has the legal authority to suspend e-commerce businesses in certain cases. The FTC Chairman, Ju Biung-ghi, went on record saying "all available means" would be considered, including a full or partial business suspension of Coupang, depending on the investigation outcome. Under Korea's Act on Consumer Protection in Electronic Commerce, the KFTC can order a company to "fully or partially suspend business" for up to 6 months (extendable to 1 year). However, this draconian step is legally reserved for situations where a company either *repeatedly* violates the law or fails to comply with corrective orders such that consumer harm cannot otherwise be prevented.

Despite the tough talk, a full business suspension of Coupang is viewed as highly unlikely in practice. Legal experts and precedent suggest regulators will hesitate to wield this "nuclear option". Professor Choi Kyoung-jin, a law expert who heads the Personal Data Professionals Association, noted that while a temporary suspension is *legally* possible, "it doesn't look easy for Coupang to get a business suspension" in reality.

There are several reasons: (1) Legal criteria not clearly met: The law requires either repeated violations or failure to follow corrective measures. Coupang's breach, though massive, was a single incident. The company had prior minor data lapses (in 2021 and 2023), but those resulted in small fines and were not in the same league. Unless evidence shows Coupang willfully ignored security obligations, it's hard to classify this as a deliberate or repeated law-breaking scenario that merits a shutdown. (2) Consumer harm vs. remedy: The FTC Chairman himself acknowledged that if suspending Coupang would "result in greater harm to consumers", regulators could choose a penalty fine instead. A suspension would punish Coupang, but also punish millions of customers who rely on its services daily. Moreover, thousands of SME merchants in Korea rely on Coupang to reach its huge consumer base. If Coupang's operations were suspended, many of these merchants would likely go out of business and the regulators would be blamed. (3) Precedent of leniency: Korean regulators have so far *never* imposed a business suspension on a major tech or retail company for a data breach or consumer protection issue. A telling precedent came in 2024: the KFTC considered suspending the game company Nexon for six months over a loot-box scandal, but opted to fine ₩11.5 billion rather than inconvenience millions of gamers. Coupang's scale is far larger than Nexon's, tilting the balance even more toward fines over suspension. (4) Political-economic considerations: Coupang is a flagship of Korean e-commerce and a U.S.-listed company. A suspension could provoke criticism that Korea is undermining its own digital economy and unnecessarily harming US investors.

Taking these factors together, the consensus among analysts is that the suspension threat is mostly a pressure tactic, a way to ensure Coupang fully complies with investigations and offers generous redress to users. The regulators have essentially confirmed as much: KFTC Chairman Ju said enforcement will depend on proving actual consumer financial harm, and that if Coupang makes victims whole, a suspension might not be necessary. As of now, there's no evidence of widespread financial losses from the leaked data (since no payment info was leaked). Thus, barring new damaging revelations, the probability of an actual suspension order is very low. Regulators are far more likely to hit Coupang with strict corrective orders and monetary penalties while allowing it to continue operating.

If, in a highly unlikely scenario, the authorities did issue a suspension order, Coupang would almost certainly fight it through legal channels. Under Korean law, companies can file an administrative lawsuit to challenge regulatory sanctions. There is precedent for Korean courts overturning or reducing KFTC actions: for example, in 2022 the Supreme Court upheld a reversal of KFTC sanctions against an airline company. Additionally, SK Telecom's initial ₩370 billion fine for its data breach was reduced to ₩134.8 billion on appeal and negotiation. In summary, Coupang is not defenseless: the company can use Korea's legal system to mitigate

regulatory actions. From an investor standpoint, the extreme regulatory scenarios (e.g. losing its business license) remain a very low-probability tail risk.

3. Financial Impact & Liquidity Stress Test

Cost Quantification

The data breach is set to cost Coupang a substantial sum: potentially into the billions of dollars when all direct and indirect costs are tallied.

The first major cost component is customer redress. Coupang announced it will spend ₩1.685 trillion (approximately $1.17 billion) on a compensation program for affected users. This is by far the largest compensation for a breach in Korean history, over three times larger than the package SK Telecom offered after its data leak earlier in 2025. Coupang's plan provides each of the 33.7 million current, former, or even deleted-account users with ₩50,000 worth of vouchers (split across its various services). While generous in aggregate, these are not cash payouts but coupons to be used on Coupang's platforms, a fact that has drawn cynicism (the compensation effectively funnels customers back into Coupang's ecosystem). Nonetheless, from an accounting perspective, this ₩1.68 trillion is a real cost (foregone revenue or additional expense) that will hit Coupang's financial statements.

The second major cost will be regulatory fines. Under the Personal Information Protection Act (PIPA), the PIPC can fine a company up to 3% of the relevant revenue for a data breach. Korean media have reported that Coupang faces a potential fine in the order of ₩1 trillion (~$770 million). However, PIPC has historically come in well below the statutory maximum. There's also litigation risk: class-action-style lawsuits could emerge, though in Korea these tend to be smaller in scale.

We should also consider the cost of IT remediation: Coupang will have to invest heavily to upgrade its cybersecurity (as promised by the CEO). For context, SK Telecom committed ₩700 billion (over $500M) over 5 years on data security enhancements after its breach. A significant capital expenditure and operating cost increase on security is likely.

In total, if we combine: roughly $1.17B in vouchers, perhaps $500M–$800M in fines (mid to high estimate), maybe $50M+ in legal settlements down the line, and say $200M–$300M in extra security and other costs (spread over years), we could be looking at around $2 to $2.5 billion USD in cumulative impact. That's approximately 2 times Coupang's Last Twelve Months free cash flow. So the breach essentially wipes out one or two years' worth of profitability in extra expenses. However, Coupang's financial position can withstand this.

Affordability (Can Coupang Absorb the Costs?)

Despite the eye-popping sums above, Coupang's balance sheet and cash flows suggest it can absorb these costs without existential strain. As of the end of Q3 2025, Coupang held approximately $7.3 billion in cash and cash equivalents (including restricted cash). This war chest (on the order of ₩9–10 trillion) largely stems from its IPO proceeds and retained earnings from recent profitable quarters. In addition, Coupang's business has turned the corner on profitability and cash generation. Over the 12 months up to Q3 2025, Coupang produced $1.2 billion in free cash flow (around ₩1.6–1.7 trillion), and operating cash flow of $2.4B. It had also achieved a small net profit for the first three quarters of 2025 (around $95M net in Q3 alone). This means the company is no longer burning cash; it's adding to its coffers each quarter.

Given those figures, let's stress test: ₩1.68 trillion in user vouchers is an obligation, but it's not a pure cash expense upfront – these vouchers will be used over time. Together, compensation +

a top-end fine (~₩2.68T) consume roughly 30% of Coupang's cash reserves. That leaves a very substantial buffer. And if the fine comes in lower (say ₩300B), the cash hit is proportionally smaller. Coupang's liquidity ratios will remain healthy. It has no pressing debt maturities that would conflict with these payouts.

In summary, Coupang can afford to pay for its mistakes. The company's strong cash position and positive cash flow mean it should comfortably meet compensation commitments and regulatory penalties. It might result in a couple of quarters of losses or lower earnings (essentially absorbing these costs), but not a liquidity crunch. This financial resilience is a key reason why the investment community has not written off Coupang – the risk is more about reputation and growth, not about bankruptcy or capital shortfall.

4. Comparative Analysis

Korean Peer Comparison – SK Telecom Breach (2025)

The closest Korean parallel to Coupang's breach is the SK Telecom data leak that was disclosed in April 2025. As Korea's largest mobile carrier, SKT holds personal data for tens of millions, making it akin to Coupang in scale of user base. In SKT's case, a malware attack on its systems led to the compromise of 26.96 million pieces of user data, impacting about 23.24 million individuals. Regulators labeled SKT's security "negligent": the Ministry of Science and ICT found SKT hadn't adequately protected customer data, violating its duty of care.

However, the regulatory response provides a blueprint of what happens to a "too big to suspend" company in Korea. The government did not suspend SK Telecom's operations at all (telecom being an essential service). Instead, they focused on penalties and remediation. SKT was hit with a fine initially calculated at ₩370 billion, but after mitigation it ended up being ₩134.8 billion (roughly $100M) – the largest privacy fine in Korean history until that point. Additionally, the Ministry of ICT imposed a modest ₩30 million administrative fine and ordered SKT to enhance security measures quarterly and have the CEO oversee data protection directly.

SK Telecom's management response was proactive: CEO Ryu Young-sang apologized promptly and the company announced a huge customer compensation plan on its own initiative. Specifically, SKT offered a 50% discount on one month's telecom bill for all 24 million customers as a form of compensation, valued around ₩500 billion (roughly $350M) in total. They also provided free USIM card replacements to all customers to mitigate any security risk. In parallel, SKT committed to investing ₩700 billion over five years to upgrade its cybersecurity infrastructure. These gestures were seen as taking responsibility and helping rebuild trust. Importantly, no mass customer exodus occurred – SKT did not report a major wave of subscribers switching to competitors.

In summary, SK Telecom's breach is a reassuring precedent for Coupang investors: the company remained fully operational, took a known financial hit, and moved on. Coupang can hope to emulate that trajectory, paying a big fine and compensation now, but continuing to dominate e-commerce thereafter. One caveat: Coupang's breach has higher profile and arguably more public anger due to perceived mishandling, so the intangible reputational damage might be greater. But financially and regulatorily, the SKT pattern of fines-not-forced-closure seems to be holding.

Global Benchmarks

Looking beyond Korea, several major breaches of tech/platform companies show how regulatory actions and business impact can play out. Equifax (2017) had ~147 million people's

sensitive info stolen and faced a global settlement of up to $700 million. Its stock plunged over 30% in the weeks after the breach, wiping out $5+ billion in market cap. However, in the years following, Equifax's stock gradually recovered and even surpassed pre-breach levels as the company improved security and the credit reporting oligopoly remained intact. Facebook/Cambridge Analytica (2018) led to a $5 billion FTC fine, one of the largest ever. Despite #DeleteFacebook trends, Facebook's user base did not significantly shrink; monthly active users continued to grow even amid bad press. The stock initially dropped ~20% during the revelation of the scandal in 2018, but within a year or so had rebounded strongly.

In all these global cases, a pattern emerges: fines and settlements can reach into the hundreds of millions or even billions, but companies rarely suffer long-term consumer exodus. The stock recovery time varied – sometimes a few months, sometimes a couple of years – but investors eventually recognized that the core business hadn't vanished. From an investment perspective, the global evidence suggests the breach will be a significant one-time cost and a temporary reputational overhang, but not a permanent impairment to user metrics or growth.

5. Investment Thesis & Valuation Impact

Effect on Structural Thesis Drivers

Before the breach, our bull case for Coupang (see deep dive here) centered on several key drivers:

- **Rocket WOW Membership Lock-in:** Coupang's subscription program (Rocket WOW) and its ecosystem (Rocket Delivery, Coupang Eats, Coupang Play streaming, etc.) created high customer stickiness. Users paying for WOW were ordering more frequently due to free delivery and enjoying bundled services, making them less likely to churn to competitors.
- **Scale Moat and Cost Advantages:** Coupang's massive scale, with over 24 million active customers and a dense logistics network, gave it economies of scale that competitors couldn't easily match. This virtuous cycle (more buyers and sellers attracting each other, larger volume lowering per-unit costs) was a core moat.
- **Management Quality and Execution:** We previously praised Coupang's management (especially founder Bom Kim) for vision and effective execution, turning Coupang into a dominant "Amazon of Korea" with a track record of innovation and prudent capital allocation.

Now, the data breach poses challenges to each of these drivers, though some more than others.

Rocket WOW Lock-in

Initially, one might fear the breach would break the bond between Coupang and its loyal customers. Indeed, there was an immediate spike in WOW cancellations and user outrage post-disclosure: users flooded online forums with vows to cancel memberships and some did leave. Coupang's daily active user count did dip in December (DAUs fell into the 14 million range from the usual 15–16 million). However, the decline in users appears to be relatively modest given the scale of the incident. Many longtime WOW members found it hard to actually quit. Why? Because the convenience and value provided by Coupang still outweighed the single (albeit serious) lapse. As one user was quoted: "Coupang's handling looks bad… but I've continued using Coupang even after the breach". Another user explicitly said "Rocket WOW delivery is the reason I can't leave Coupang", as they rely on it for personal and work purchases

on a weekly basis. These anecdotes, supported by usage data, show that the lock-in effects are intact: users have integrated Coupang into their lives (from daily essentials to entertainment via Coupang Play), and alternatives don't offer the same one-stop convenience.

Scale Moat

Coupang's scale moat and cost advantages are fundamentally operational, driven by its logistics network, fulfillment infrastructure, and the marketplace's breadth of selection. These advantages remain largely untouched. None of the breach information suggests any issue with Coupang's fulfillment or logistics capabilities. In fact, during the scandal, Coupang's operations continued normally, packages still arrived on time. Coupang's scale in logistics and selection is intact, and rivals haven't suddenly grown larger; if anything, Coupang's lead remains, and it's now pouring money into security which smaller rivals might struggle to match. The breach did not introduce new competition: e-commerce in Korea is still essentially Coupang vs a distant second (Naver Shopping). The long-term competitive positioning in the market remains as it was.

Management Quality

This is where the thesis takes a hit. Post-breach, some investors will question management's judgment and transparency. Bom Kim's handling of the crisis, waiting over a month to apologize, not appearing at hearings, has drawn criticism not just in Korea but also from foreign investors who value strong governance. The breach has revealed a possible blind spot in Coupang's management: a fast-growing tech firm that may have underinvested in risk management and public relations. We are disappointed with the initial response to the crisis from Coupang's management. That said, management quality can be re-earned. Bom Kim eventually did the right things (apologized, promised improvements, and presumably green-lit a huge compensation package that puts customers first financially). We also saw Coupang swiftly identify the culprit and cooperate with authorities to recover data: that speaks to a competent technical response once the breach was known. The breach might actually refocus management on operational excellence (they can ill afford another major mistake). For now, one might adjust the thesis to say: Coupang's management is excellent at growth and operations, but has shown weakness in crisis management, a risk factor to monitor.

In sum, the structural drivers of Coupang's investment case remain fundamentally in place: its customer base is still huge and largely loyal, its competitive moat in logistics and selection is unshaken, and the long-term secular trend (shift to e-commerce) hasn't changed. The breach imposes a one-time financial cost and a need for reputation repair, but it doesn't dismantle the business model. It does, however, highlight new risk factors (data security, regulatory intervention) that investors will price into the stock to some degree.

Valuation Scenario Analysis

Before the breach, the base-case DCF valuation for Coupang (per our original report) was about **$40.84 per share** – implying a significant upside to the then-current trading price. Now we reassess how the breach might affect that valuation.

Most Likely Scenario: Moderate Fine + Minimal Churn. In this scenario, regulators levy a fine but it's at a moderate level, not the theoretical max. Perhaps the PIPC fine comes out to ₩300–500 billion, recognizing Coupang's cooperation and first-time nature. That would still be 2–3× the SKT fine and set a new record, but not crippling. Total regulatory penalties might be on the order of ₩400–600B (roughly $300–450M). Next, assume customer churn is minimal. Many users were upset yet remain, and those who left are perhaps offset by new customer growth resuming in 2026 (Korea's e-commerce is still expanding). We did see a temporary dip in DAUs,

but let's say by mid-2026 usage levels are back to or above pre-breach levels. Essentially, Coupang's growth trajectory remains intact, perhaps with a small delay. Under this scenario, the compensation vouchers plus improved customer outreach could actually strengthen loyalty among some users (they feel they got something back). The financial impact is then largely one-off: the ₩1.68T vouchers and a ₩X fine. These would reduce 2025-26 cumulative cash flow, but have no effect on long-term growth rates or margins beyond 2026. The DCF valuation in this scenario would be only marginally lower than pre-breach. We might shave perhaps 5% off the intrinsic value to account for the net present cost of fines/comp and perhaps a slight increase in the equity risk premium due to perceived governance risk. If base was ~$40/share, we might now say base-case is ~$38.

Downside Scenarios: In a more severe scenario (high fine + higher customer churn but no suspension), Coupang's 2026 revenue growth might stall as lost volume from churn offsets organic growth. The company would then have to re-acquire those customers over time, meaning increased marketing and promotions expense in 2026–27. We could dial down the long-term revenue CAGR in the DCF from 14% to perhaps 8-10%. A rough estimate: perhaps 10-20% lower valuation than base case, yielding somewhere in the low- to mid-$30s per share. The core investment thesis (dominant platform) would be dented but not destroyed.

In the extremely unlikely "nightmare scenario" (massive fine + business suspension), the impact would be severe – potentially 30-50% lower than base case. However, as discussed, this scenario is a very low-probability tail risk.

Our Assessment: We believe the most likely outcome is the moderate scenario (or a mild variant of the downside scenario) given current information. The Korean authorities have signaled they want to punish but not cripple the company, and user behavior data so far shows inconvenience and anger, but not mass abandonment. Coupang's weekly active users actually *increased* the week after the breach disclosure (likely due to users logging in to check their data or change settings), showing that people didn't immediately abandon the platform en masse.

Long-term Risk/Reward Profile

The breach does alter the risk profile – mainly by adding a new dimension of regulatory and reputational risk – but does not significantly diminish the reward profile if managed properly. The upside scenario (aggressive growth/margins) might be pushed out by a year or two, but could still be reachable if Coupang continues to consolidate e-commerce and expands internationally. The "time to thesis" is delayed: before, investors might have expected accelerating profits in 2025-2026, whereas now 2026 might be a "recovery year" with extra costs, with the real inflection coming 2027 once breach costs are fully past.

The breach has been a harsh test of Coupang's resilience – and so far, it appears the company will **pass that test**, albeit with some scars. For long-term investors, the core appeal of Coupang (its scale, growth runway, and potential for Amazon-like dominance) is fundamentally unchanged, while the stock's volatility around this event has been more about sentiment and uncertainty. Once clarity arrives (likely aligning with the moderate scenario), the focus can return to growth and execution, and the valuation should gradually reflect the strong reward side of the equation once more.

As the stock is down ~25% as a result of the crisis and our thesis and valuation remain largely intact, we believe the gap between the current share price and intrinsic value has widened attractively.

Our Decision: Adding to Our Position

Given the analysis above, we have decided to add to our Coupang position in the model portfolio at current levels. Our rationale:

1. **The structural thesis is intact.** The breach was a serious operational lapse but did not damage Coupang's core competitive advantages – its logistics network, scale economies, and ecosystem lock-in remain undiminished.

2. **Financial impact is manageable.** With $7.3B in cash and $1.3B in annual free cash flow, Coupang can absorb the ~$2B cumulative cost without liquidity stress.

3. **Regulatory tail risk is very low.** The suspension threat appears to be leverage, not intent. Precedent (SK Telecom, Nexon) strongly suggests fines, not shutdowns.

4. **Valuation has become more attractive.** The stock is down ~25% on news that warrants perhaps a ~5% reduction in intrinsic value under the most likely scenario. This creates a wider margin of safety for long-term investors.

5. **User stickiness is holding.** Early data shows DAU declines in the single digits, not the mass exodus one might fear from the largest data breach in Korean history. Rocket WOW lock-in is proving resilient.

We recognize that governance risk has increased and will monitor management's follow-through on promised security improvements and regulatory cooperation. However, the risk/reward at current prices, weighted for scenario probabilities, has improved compared to pre-breach levels.