UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K/A
(Amendment No. 1)

CURRENT REPORT
Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934

December 15, 2025
Date of Report
(Date of earliest event reported)

COUPANG, INC.

(Exact name of registrant as specified in its charter)

Delaware	**001-40115**	**27-2810505**
(State or other jurisdiction of incorporation or organization)	(Commission File Number)	(I.R.S. Employer Identification Number)

720 Olive Way, Suite 600
Seattle, Washington 98101
(Address of principal executive offices, including zip code)

(206) 333-3839
(Registrant's telephone number, including area code)

Not Applicable
(Former name or former address, if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Trading Symbol(s)	Name of Each Exchange on Which Registered
Class A Common Stock, par value $0.0001 per share	CPNG	New York Stock Exchange

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (17 CFR §230.405) or Rule 12b-2 of the Securities Exchange Act of 1934 (17 CFR §240.12b-2).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 1.05. Material Cybersecurity Incidents.

On December 24, 2025 (PST) and December 28, 2025 (PST), Coupang Corp., a wholly-owned Korean subsidiary (“Coupang Corp.”) of Coupang, Inc. (“Coupang, Inc.,” “our,” or “we”) (Coupang Corp., together with Coupang, Inc. and its subsidiaries and affiliates, “Coupang,”), issued updates (collectively, the “Updates”) on the cybersecurity incident (the “Incident”) disclosed in the Current Report on Form 8-K filed by Coupang, Inc. with the U.S. Securities and Exchange Commission (the “SEC”) on December 16, 2025. The Updates provided, in part, that the perpetrator of the Incident has been identified, is cooperating with Coupang and investigators, and has turned over all devices used in the Incident. Further, the investigation to date indicates that while approximately 33 million accounts were accessed, the perpetrator only saved limited data from approximately 3,000 customer accounts, and such customer data has been deleted without having been shared with a third party. In addition, Coupang Corp. announced a customer compensation program to issue approximately 1.685 trillion won (approximately $1.2 billion) worth of vouchers, starting January 15, 2026, to customers who were notified of the Incident at the end of November 2025 that may be applied towards future Coupang purchases. These vouchers will be reflected as reductions to the selling price and revenue recognized on each corresponding transaction.

Item 7.01. Regulation FD Disclosure.

The investigation regarding the Incident is ongoing. Copies of the Updates are furnished as Exhibit 99.1 to this Current Report on Form 8-K/A. In addition, as part of our ongoing commitment to transparency to our investors, customers, and other stakeholders, we may provide additional updates regarding the Incident and relevant developments at: https://www.aboutcoupang.com or https://news.coupang.com.

In accordance with General Instruction B.2 of Form 8-K, the information in this Item 7.01 and Exhibit 99.1 shall not be deemed to be “filed” for purposes of Section 18 of the Securities Exchange Act of 1934, as amended (the “Exchange Act”), or otherwise subject to the liability of that section, and shall not be incorporated by reference into any registration statement or other document filed under the Securities Act of 1933, as amended, or the Exchange Act, except as shall be expressly set forth by specific reference in such filing.

The information that can be accessed through hyperlinks or website addresses included in this Current Report on Form 8-K/A is deemed not to be incorporated in or part of this report.

Forward-Looking Statements

This Current Report on Form 8-K/A contains “forward-looking statements” within the meaning of the “safe harbor” provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, express or implied statements regarding our expectations regarding our ability to assess the Incident and its impact on Coupang, its customers, operations, and financial results. In some cases, you can identify forward-looking statements because they contain words such as "anticipate," "believe," "contemplate," "continue," "could," "estimate," "expect," "intend," "may," "plan," "potential," "predict," "project," "should," "target," "toward," "will," "shall," "remains," "goal," "objective," "seek," "strategy," "transform," "restore," "future," "opportunity," "runway," “trajectory," or "would," and the negative of these words or other similar terms or expressions. Such forward-looking statements include, but are not limited to, statements regarding the nature and scope of the Incident, the ongoing investigations regarding the Incident, the impact of the Incident on Coupang, its customers, operations, and financial results, and the customer compensation program and its accounting treatment. Actual results and outcomes could differ materially for a variety of reasons, including, among others, Coupang’s ongoing assessment of the impacts of the Incident, including the potential discovery of additional information related to the Incident; Coupang’s expectations regarding its ability to contain and remediate the Incident; the magnitude of the potential disruption to Coupang’s business and operations; the impact of the Incident on Coupang’s relationships with customers, employees, merchants, suppliers, advertisers, investors, regulators and governmental authorities; legal, reputational, and financial harm that may result from the Incident, including financial penalties and litigation awards or settlements that may arise from regulatory investigations or litigation in connection with the Incident; distraction of management or other diversion of resources from business operations caused by the Incident; and the potentially material financial impact of the potential loss of revenue and potential higher expenses, including from remediation, regulatory penalties, litigation, customer compensation, or other additional expenses that may be incurred or borne by Coupang in connection with the Incident. Coupang is also subject to other risks and uncertainties. For additional information on other potential risks and uncertainties that could affect Coupang, please see our most recent Annual Report on Form 10-K and subsequent SEC filings. All forward-looking statements in this report are based on information available to Coupang and assumptions and beliefs as of the date hereof, and Coupang disclaims any obligation to update any forward-looking statements, except as required by law. You should not place undue reliance on our forward-looking statements.

Item 9.01 Financial Statements and Exhibits.

(d) Exhibits.

Exhibit Number	Description of Exhibit
99.1	Updates on Coupang Corp. (Korean Subsidiary) Cybersecurity Incident
104	Cover Page Interactive Data File (formatted as inline XBRL and contained in Exhibit 101)

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

COUPANG, INC.

By:	/s/ Harold L. Rogers
Name:	Harold L. Rogers
Title:	General Counsel and Chief Administrative Officer

Dated: December 29, 2025

Update on Coupang Korea Cybersecurity Incident

Below are the statements Coupang published related to the recent cybersecurity incident.

Originally posted on Dec 29, 2025 09:50 in KST:

– Coupang Announces Compensation Plan to Restore Customer Trust . . . Issuing 1.685 Trillion Won Worth of Purchase Vouchers

– Compensation plan implemented for all 33.7 million customers . . . To be provided sequentially starting January 15, next year

– Equivalent to 50,000 won per person . . . Purchase vouchers for all Coupang products and for Coupang Eats, Travel, and R.LUX

– Practicing 'customer-centric principles' . . . We will transform into a company trusted by customers.

Fully acknowledging its responsibility for the recent personal information leak incident, Coupang announced on the 29th that it plans to implement a 1.685 trillion won customer compensation plan to restore customer trust.

Harold Rogers, Coupang Corp.'s interim CEO, stated, "All Coupang executives and employees deeply regret the significant concern and distress the recent personal data leak has caused our customers," adding, "We have prepared a compensation plan as part of taking responsible action for our customers."

Coupang plans to distribute purchase vouchers worth around 1.685 trillion won to customers starting January 15 next year. The plan applies to 33.7 million customer accounts who were notified of the personal information leak at the end of last November. Purchase vouchers will be provided equally to both WOW and non-WOW members. It also includes Coupang customers who had canceled their membership and were notified of the personal data leak. The company plans to sequentially notify its 33.7 million customer accounts via text message about the use of the purchase vouchers.

Coupang will provide each customer with four single-use purchase vouchers totaling 50,000 won: all Coupang products including Rocket Delivery, Rocket Overseas, Seller Rocket, and Marketplace (5,000 won), Coupang Eats (5,000 won), Coupang Travel products (20,000 won), and R.LUX products (20,000 won).

Customers can check the purchase vouchers sequentially on the Coupang app starting January 15 and apply them when purchasing products. More specific details are scheduled to be released in a separate announcement.

Harold Rogers, Coupang Corp.'s interim CEO, stated, "Taking this incident as a turning point, Coupang will wholeheartedly embrace 'customer-centric principles' and fulfill its responsibilities to the very end, transforming into a company that customers can trust," adding, "We once again deeply apologize to our customers."

Originally posted on Dec 26, 2025 15:00 in KST:

Coupang's investigation was not a "self investigation." It was an investigation coordinated on a daily basis, under the express direction of government, over a period of several weeks.

This data leak incident has caused great concern to the public and the continued misstatements that Coupang was conducting an investigation without governmental oversight are creating false insecurity. We would like to clarify facts of our coordination process with the government.

On December 1, the government approached Coupang and asked for full cooperation.

On the 2nd, Coupang received an official, written letter with regard to the incident from the government. On an almost daily basis for the next several weeks, Coupang worked with the government to locate, contact, and communicate with the leaker. At the direction of the government, Coupang secured the leaker's full confession, recovered all devices used in connection with the leak, and received critical details about Coupang user information. As soon as Coupang received new facts, sworn testimony, or physical materials from the leaker, Coupang turned them over to the government immediately.

On the 9th, the government suggested that Coupang contact the leaker. Coupang worked with the government on messaging and word choice in its communications. Following this, Coupang met the leaker initially on the 14th and reported this to the government. On the 16th, we completed the primary retrieval of the leaker's desktop and hard drives as directed by the government, which was then reported. On the 17th, we provided them to the government. Coupang understands that after it delivered the hard drive to the government, the government began an immediate review. The government then requested that we recover additional devices from the leaker.

On the 18th, Coupang recovered the leaker's MacBook Air laptop from a nearby river. Coupang used a forensics team to document and take inventory and then immediately handed the laptop over to the government. On December 21 the government let Coupang to deliver the hard drives, laptop, and all three sworn and fingerprinted declarations to the police. At all times Coupang obeyed the government's order to keep the operation confidential and not disclose any details, even while governmental agencies, the National Assembly, and parts of the media falsely accused Coupang of failing to seriously address the leak.

On the 23rd, at the government's request we provided additional briefing about the details of the investigation including details about Coupang's cooperation with the government. Subsequently, on the 25th, we notified Coupang customers of the investigation status.

Coupang will fully cooperate with the ongoing government investigation and take all necessary measures to prevent any secondary harm.

Timeline of Government Coordination to Recover Leaked Information

Date	Timeline of Government Coordination
December 1	Coupang met with the government and agreed full cooperation.
December 2	Coupang received an official, written letter with regard to the incident from the government.
December 9	The government proposed that we contact the leaker directly
December 14	Meeting with the leaker for the first time and reported the meeting to the government.
December 16	We reported to the government that the leaker's devices (the desktop computer's hard drives) had been recovered.
December 17	We delivered the leaker's devices (the desktop computer's hard drives) and a written statement to the government, and the government began to process those materials that day.
December 18	An additional device belonging to the leaker (a laptop) was recovered from the river and handed over to the government. In addition, the government requested that we secure the leaker's fingerprints on every previously signed document, which we did.
December 21	The government authorized Coupang to submit all materials (sworn statements, lap top, hard drives) to the police. The leaker's devices were provided to the police for forensic analysis.
December 23	We submitted and briefed the government on a detailed report outlining the relevant developments.
December 25	Customers were informed of the investigation results.
December 26	We provided another briefing to a governmental agency.

Timeline of Government Coordination to Recover Leaked Information

Originally posted on Dec 25, 2025 15:35 in KST:

Coupang confirmed that the perpetrator has been identified, and that all devices used in the data leak have been retrieved. The investigation to date indicates that the perpetrator retained limited user data from only 3,000 accounts and subsequently deleted the user data.

Based on the investigation to date:

- The perpetrator accessed 33 million accounts, but only retained user data from approximately 3,000 accounts. The perpetrator subsequently deleted the user data.
- The user data included only 2,609 building entrance codes. No payment data, log-in data or individual customs numbers
- The perpetrator never transferred any of the data to others

We know the recent data leak has caused concern among our customers, and we apologize for the anxiety and inconvenience. Everyone at Coupang and the government authorities has been working tirelessly together to address this critical issue, and we are now providing an important update.

Coupang used digital fingerprints and other forensic evidence to identify the former employee who leaked user data. The perpetrator confessed everything and revealed precise details about how he accessed user data.

All devices and hard drives the perpetrator used to leak Coupang user data have been retrieved and secured following verified procedures. Starting from the submission of the perpetrator's declaration to government officials on December 17, Coupang has been submitting all devices including hard drives to government officials as soon as we received them. Coupang has also been cooperating fully with all relevant ongoing government investigations.

From the beginning, Coupang commissioned three top global cybersecurity firms—Mandiant, Palo Alto Networks, and Ernst & Young—to perform rigorous forensic investigation.

The investigative findings to date are consistent with the perpetrator's sworn statements: (i) that he accessed basic user data from 33 million customer accounts using a stolen security key, (ii) that he only retained user data from roughly 3,000 total accounts (name, email, phone number, address and part of order histories), (iii) that from the roughly 3,000 accounts, he only retained 2,609 building entrance access codes, (iv) that he deleted all stored data after seeing news reports of the leak, and (v) that none of the user data was ever transmitted to others.

1. **Perpetrator accessed basic user data using a stolen security key.** The perpetrator stated that he was able to access limited user data—including names, emails, addresses, phone numbers—by stealing an internal security key that he took while still working at the company. Data logs and forensic investigation had already confirmed that the access was carried out using a stolen internal security key and included only the types of data the perpetrator specified (e.g., names, emails, addresses, phone numbers). He did not access any payment data, log-in data, or individual customs numbers.

2. **Perpetrator gained very limited access to order history and building entrance codes.** The perpetrator stated that while accessing basic data relating to a large number of customers, he only ever accessed the order history and building entrance codes for roughly 3,000 accounts. Independent forensic analysis of data logs had already determined that the number of building entrance codes for only 2,609 were ever accessed, just as the perpetrator reported.

3. **Perpetrator used a desktop PC and MacBook Air laptop for the attack.** The perpetrator stated that he used a personal desktop PC and a MacBook Air laptop to provision access and to store a limited amount of user data. Independent forensic investigation confirmed that Coupang systems were accessed using one PC system and one Apple

system as the primary hardware interfaces, exactly as the perpetrator described. The perpetrator relinquished the PC system and four hard drives used on the PC system, on which analysts found the script used to carry out the attack.

4. **Perpetrator sought to erase and dispose of the MacBook Air laptop in a river.** The perpetrator stated that when news outlets reported on the data leak he panicked and sought to conceal and destroy the evidence. Among other things, the perpetrator stated that he physically smashed his MacBook Air laptop, placed it in a canvas Coupang bag, loaded the bag with bricks, and threw the bag into a nearby river. Using maps and descriptions provided by the perpetrator, divers recovered the MacBook Air laptop from the river. It was exactly as the perpetrator claimed—in a canvas Coupang bag loaded with bricks—and its serial number matched the serial number in the perpetrator's iCloud account.

5. **Perpetrator retained a very small amount of user data, never transferred any of the data, and subsequently deleted all the stored user data.** The perpetrator stated that he worked alone, that he only retained a small amount of user data from roughly 3,000 accounts, that the user data was only ever stored on his personal desktop PC and MacBook Air laptop, that none of that user data was ever transmitted to a third party, and that he deleted the stored data immediately after seeing news reports of the leak. The investigative findings to date are consistent with the perpetrator's sworn statements and found no evidence that contradicts these statements.

We will provide updates following the investigation and plan to separately announce compensation plans to our customers in the near future.

Coupang remains fully committed to protecting customer data. We will cooperate fully with the government's investigation, take all necessary steps to prevent further harm, and strengthen our measures to prevent recurrence.

Coupang regrets the concern this incident has caused and apologizes to those affected.