coupang newsroom

쿠팡은 유출자를 특정하였고, 고객 정보 유출에 사용된 모든 장치가 회수되었음을 확인하였습니다. 현재까지 조사에 의하면, 유출자는 약 3,000개 계정의 제한된 고객 정보만 저장했고, 이후 이를 모두 삭제하였습니다.

2025. 12. 25.

쿠팡은 유출자를 특정하였고, 고객 정보 유출에 사용된 모든 장치가 회수되었음을 확인하였습니다. 현재까지 조사에 의하면, 유출자는 약 3,000개 계정의 제한된 고객 정보만 저장했고, 이후 이를 모두 삭제하였습니다.

현재까지 조사에 의하면,

- 유출자, 3300만 고객 정보 접근했지만 약 3000개 계정만 저장하였고, 이 역시 모두 삭제하였음
- 저장한 고객 정보는 공동현관 출입번호 2609개 포함. 다만, 결제정보·로그인·개인통관고유번호는 없음
- 외부 전송 등 추가 유출 없음

최근 발생한 개인정보 유출이 고객들에게 얼마나 큰 우려를 불러일으켰는지 책임을 통감합니다. 쿠팡 개인정보 유출 사태로 인해 수많은 국민들이 걱정과 불편을 겪게 된 것에 대해 진심으로 사과드립니다. 이 사태를 책임감 있게 수습하기 위해 정부기관과 쿠팡의 전 구성원들이 함께 최선의 노력을 다했고, 중요한 업데이트 내용을 상세히 설명드립니다.

쿠팡은 디지털 지문(digital fingerprints) 등 포렌식 증거를 활용해 고객 정보를 유출한 전직 직원을 특정했습니다. 유출자는 행위 일체를 자백하고 고객 정보에 접근한 방식을 구체적으로 진술했습니다.

유출자가 쿠팡 고객 정보를 접근 및 탈취하는 데 사용된 모든 장치와 하드 드라이브는 검증된 절차에 따라 모두 회수되어 안전하게 확보되었습니다. 쿠팡은 지난 12월 17일 유출자의 진술서 제출을 시작으로, 관련 장치 등 일체 자료를 확보하는 즉시 정부에 제출해 왔습니다. 쿠팡은 현재 진행 중인 정부기관의 관련 조사에도 성실히 협조해 왔습니다.

사건 초기부터, 쿠팡은 엄격한 포렌식 조사를 진행하기 위해서 전세계 최상위 3개 글로벌 사이버 보안 업체인 맨디언트, 팔로알토 네트웍스, 언스트앤영에 조사를 의뢰했습니다.

현재까지 조사 결과는 유출자의 진술 내용과 부합합니다. 이에 의하면, 1) 유출자는 탈취한 보안 키를 사용하여 3,300만 고객 계정의 기본적인 고객 정보에 접근했고, 2) 약 3,000개 계정의 고객 정보(이름, 이메일, 전화번호, 주소, 일부 주문정보)만 실제 저장했으며, 3) 여기에 포함된 공동현관 출입번호는 2,609개였고, 4) 사태에 대한 언론보도를 접한 후 저장했던 정보를 모두 삭제했으며, 5) 고객 정보 중 제3자에게 전송된 데이터는 일체 없습니다.

1. 유출자는 탈취한 보안 키를 이용해 기본적인 고객 정보에 접근함

유출자는 재직 중에 취득한 내부 보안 키를 탈취해 이름, 이메일, 주소, 전화번호 등 일부 고객 개인정보에 접근했다고 진술했습니다. 데이터 로그 및 포렌식 조사를 통해, 해당 접근은 탈취된 내부 보안 키를 이용했으며, 접근된 데이터의 유형 또한 유출자가 진술한 범위(이름, 이메일, 주소, 전화번호)에 한정되었음을 확인했습니다. 결제정보, 로그인 관련 정보, 개인통관번호에 대한 접근은 없었습니다.

2. 유출자는 주문 이력 및 공동현관 출입 정보에는 매우 제한적으로 접근함

유출자는 다수 고객의 기본 고객 정보에 접근하는 과정에서 약 3,000개의 계정에 대한 주문정보와 공동현관 출입번호에 접근했다

고 진술했습니다. 독립적인 외부 전문업체의 포렌식 분석 결과, 2,609개의 공동현관 출입번호가 접근된 것으로 확인되며, 이는 유출자의 진술과 부합합니다.

3. 유출자는 데스크톱 PC와 MacBook Air노트북을 사용해 공격함

유출자는 개인용 데스크톱 PC와 MacBook Air 노트북을 사용해 공격을 시도했고 접근한 정보 중 일부를 해당 기기에 저장했다고 진술했습니다. 독립적인 포렌식 조사 결과 쿠팡 시스템에 대한 불법접근은 유출자가 진술한 대로 1대의 PC 시스템과 1대의 애플 시스템을 통해 수행된 것으로 확인됐습니다. 유출자는 해당 데스크톱 PC와 PC에서 사용된 4개의 하드 드라이브를 제출했으며, 분석 결과 이들 저장장치에서 공격에 사용된 스크립트가 발견됐습니다.

4. 유출자는 MacBook Air노트북을 삭제 및 파기하기 위해 하천에 투기했음

유출자는 언론을 통해 데이터 유출 보도가 나오자 극도의 불안 상태에 빠져 증거의 은폐·파기를 시도했다고 진술했습니다. 유출자는 MacBook Air 노트북을 물리적으로 파손한 뒤 쿠팡 로고가 있는 에코백에 넣고 벽돌을 채워 인근 하천에 던졌다고 진술했습니다. 유출자가 제공한 지도와 설명을 바탕으로 잠수부들이 해당 하천에서 MacBook Air 노트북을 회수했으며, 회수된 기기는 유출자의 진술 그대로 "벽돌이 담긴 쿠팡 에코백" 안에 들어 있었고, 일련번호 또한 유출자의 iCloud 계정에 등록된 일련번호와 정확히 일치했습니다.

5. 유출자는 소량의 고객 정보만 저장했으며, 외부 전송은 없었고 이후 모두 삭제했음

유출자는 단독으로 이를 저질렀으며, 약 3,000개 계정의 제한적인 고객 정보만을 저장했고, 해당 고객 정보는 개인 데스크톱 PC와 MacBook Air 노트북에만 저장됐으며 외부로 전송된 적은 없다고 진술했습니다. 또한 언론 보도를 접한 직후 저장돼 있던 고객 정보를 모두 삭제했다고 진술했습니다. 현재까지 조사 결과는 유출자의 진술 내용과 부합하며, 유출자의 진술과 모순되는 증거가 발견되지 않았습니다.

쿠팡은 향후 진행될 조사 경과에 따라 지속적으로 안내를 드릴 예정이며, 이번 사태로 인한 고객보상 방안을 조만간 별도로 발표할 예정입니다.

쿠팡은 앞으로도 고객들의 소중한 개인정보를 보호하기 위해 최선을 다할 것입니다. 정부 조사에 적극 협조할 것이며, 2차 피해를 예방하는 데 최선을 다하겠습니다. 아울러 금번 사태를 계기로 재발 방지를 위한 모든 방안을 강구할 것임을 약속드립니다.

모든 고객분들께 다시 한 번 진심으로 사과드립니다.

*The English version follows below.

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.

취재 문의 media@coupang.com