쿠팡, 사상 최대의 개인정보 유출 사태 발생

- 내부통제시스템의 실패와 잠재적인 법적 리스크

2025.12.19. 16:40 작성

2025.12.22. 11:56 수정

1. 사건의 개요

225년 11월 6일, 쿠팡 고객 약 3,370만 개 계정의 이름, 전화번호, 이메일 주소, 배송 주소, 최근 5건의 주문 이력이 유출되는 사건이 발생했다. 퇴사한 중국인 직원이 방치된 액세스 토큰 서명키를 악용하여 2025년 6월 24일부터 약 5개월간 지속된 것으로 추정된다.

쿠팡은 이번 사건 이전에도 이미 3건의 개인정보 유출 사건이 있었다. 이전의 유출 사건의 규모는 상대적으로 크지 않았던 면도 있었지만, 개인정보보호위원회가 지난 3번 사건에 대해 총 15억 9천만 원 정도의 과징금을 부과했다. 이에 대해 과징금 규모가 너무 작고, 이러한 솜방망이 처분이 이번 사태를 불러왔다는 비판도 있다. 미국과 유럽은 조 단위의 징벌적 제재를 가하고 있다.

아무튼, 쿠팡의 내부통제시스템에 문제가 있는 것으로 보인다. 특히 개인정보보호는 쿠팡 같은 이커머스 기업에게는 “Mission Critical” 즉 “핵심 비즈니스”이기에, 내부통제 실패 여부를 둘러싼 법적 공방이 치열할 것으로 보인다.

현재 국내 로펌과 미국의 로펌이 각각 한국과 미국에서 소송을 준비 중인 것으로 보도된 바 있다. 로펌들은 어떤 법적 근거를 가지고 쿠팡에 대해 책임을 물을 것인가. 이를 검토하기 전에 먼저 쿠팡의 지배구조를 이해할 필요가 있다.

한국 쿠팡은 미국 뉴욕증권거래소(NYSE)에 상장되어 거래되고 있는 Coupang Inc.의 100% 자회사이고, Coupang Inc.는 미국 델라웨어 회사법에 근거해서 설립된 미국 회사다. 따라서 한국 쿠팡의 주주는 Coupang Inc.가 유일하며, 한국에서 Coupang Inc. 주식을 보유한 한국 투자자들은 국내 증권사를 통해 NYSE에서 거래되는 미국 Coupang Inc. 주식을 매수한 것이다. 이러한 지배구조하에서 쿠팡 주식회사(이하 ‘한국 쿠팡’)와 미국 Coupang Inc.에 대한 법적 책임을 한국과 미국으로 구분해서 살펴본다.

2. 한국에서의 법적 책임 가능성

(1) 과징금 부과

한국 정부는 한국 쿠팡에 대해 개인정보보호법 위반으로 과징금을 부과할 수 있다.

과징금 규모는 위반 사고 관련 매출액의 3%까지 가능한데, 2024년 매출액 기준으로 볼 때 최대 1조 원까지도 가능한 것으로 보고 있다.
(2) 형사처벌
한국 쿠팡에 대한 벌금형도 가능하다.
(3) 행정처분
한국 쿠팡에 대한 시정명령이나 영업정지 등의 처분도 가능하다.
(4) 손해배상책임
한국 투자자들은 한국 쿠팡의 주주들이 아니기 때문에 한국 쿠팡을 대상으로 한 주주 대표소송은 불가하다. 그렇지만 정보 유출이라는 피해를 입은 고객들은 개인정보보호법 제39조를 근거로 회사를 상대로 손해배상청구는 가능하다. 또한 고객들은 상법 제401조에 근거해 이사 개인을 상대로 한 손해배상청구도 가능하다고 본다.

두 개의 소송을 비교해 볼 때, 원고 측으로서는 개인정보보호법에 근거한 소송이 직접적이고 일반적이라 할 수 있다. 동법은 개인정보처리자가 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다고 규정하여 입증책임을 전환시키고 있어서 원고에게 유리한 측면이 있고, 회사가 피고가 되기 때문에 배상 능력이 확실하다는 장점도 있다.

반면, 상법에 근거할 경우 원고 측은 한국 쿠팡 이사들의 “고의 또는 중대한 과실로 업무를 게을리했다는 점”을 증명해야 한다. 한국 쿠팡은 한국 상법에 의해 설립된 회사이므로 한국 쿠팡이 미국 회사의 100% 자회사라 하더라도 한국 상법의 지배를 받는다.

3. 미국에서의 법적 책임 가능성
(1) 이사의 감시・감독 의무 실패
한국 투자자들은 미국 델라웨어 회사법에 근거해 설립된 Coupang Inc.의 주주들이기 때문에 당연히 델라웨어 법정에서 원고적격을 갖추고 있다. 따라서 델라웨어 회사법을 근거로 Coupang Inc. 이사들의 감시・감독 의무 실패 여부를 다투게 될 것으로 보인다. 한국 로펌은 한국 투자자들을 대리해 주주 대표소송을, 미국 로펌은 미국에서 미국인 투자자들을 대리하여 주주 대표소송을 제기할 것으로 보인다.
최근 델라웨어 법원은 경영판단의 원칙의 허용 기준과 관련해서 과거와는 달리 이사들의 책임을 다소 엄격하게 묻는 판례들을 내놓고 있다. 대표적으로 2019년의 Marchand v. Barnhill 사건과 Clovis 사건, 그리고 2021년의 Boing 사건 등을 들 수 있다.

(2) 연방 증권법상 공시의무 실패
a) 민사소송
투자자들의 손해배상청구와 관련하여 중요한 소송은 연방법에 근거한 민사소송이다. 이 소송은 집단소송으로 진행될 가능성이 크다. 증권법상 Coupang Inc.의 책

임을 묻기 위해서는 “고객정보유출 사건” 관련 공시의무 위반 증명이 요구된다. 이번 사태는 포괄적 사기금지 조항인 SEC Rule 10b-5의 패턴에는 맞지 않는 것으로 보인다. 따라서 연방 증권법상 공시의무 실패 여부와 관련해서 다음의 2가지가 쟁점이 될 것으로 보인다.

첫째, 2023년 SEC는 사이버보안을 강화하면서 새로운 규칙을 제정하였는데, 등록법인의 경우 중요한 사이버 사건 발생 시 4영업일 이내에 보고의무를 부여하였다. Coupang Inc.는 이 의무를 준수하지 않은 것으로 보인다.

둘째, 등록법인은 연례 사이버 공시를 해야 하는데(Regulation S-K Item 106), 여기에는 사이버보안 위협으로부터 중요 위험을 평가・식별・관리하는 프로세스, 사이버보안 위협으로 인한 위험의 중요한 영향, 이를 담당하는 경영진의 역할과 전문성, 그리고 이사회는 사이버보안 위험을 어떻게 감독하는지가 공시 대상이다. Coupang Inc.이 이러한 규정을 준수하였는지 여부가 다투어질 것으로 보인다.

b) SEC의 제재

만약 SEC가 Coupang Inc.에 대해 SEC의 사이버보안 규칙 위반 등 다른 공시의무 위반을 근거로 민사제재금 등 제재를 내릴 수 있는데, 만약 그렇게 된다면 민사소송을 진행하는 원고 측은 커다란 힘이 될 것이다.

4. 결론

이번 쿠팡의 개인정보유출 사태는 한국 기업들이 사이버 공격에 얼마나 취약한지를 다시 한 번 보여줬다. SK텔레콤의 개인정보유출 사건이 발생한지 얼마 지나지 않아 초대형 개인정보유출 사건이 터진 것이다. 왜 한국 기업들은 내부통제시스템의 구축과 관리에 무관심할까? 왜 이커머스 기업들은 “Mission Critical”이라 할 수 있는 사이버보안 시스템 구축 및 관리에 적절한 투자를 하지 않고 있는 것일까? 약한 처벌에 과징금 조금 내는 게 더 경제적이라고 보기 때문일까?

(금융법전략연구소 김정수 대표)