제재내용 공개안

1. 금융기관명 : 롯데카드㈜

2. 제재조치일 : 2026. 7. 31.

3. 제재조치내용

제재대상	제재내용
기 관	업무 일부정지 1.5개월, 과징금 50억원
임 원	퇴직자 위법·부당사항(문책경고 수준)
직 원	퇴직자 위법·부당사항(정직 3월 수준), 정직, 감봉 3명

4. 제재대상사실

가. 금융거래의 안전성 확보의무 및 신용정보의 보호의무 위반과 이에 따른 대량 신용정보 유출

「여신전문금융업법」 제54조의4 및 제54조의5,「신용정보법」 제19조 및 제20조,「여신전문금융업감독규정」 제26조의4,「전자금융감독규정」 제14조 및 제15조 등에 의하면

신용카드업자는 신용정보전산시스템에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 기술적·물리적·관리적 보안대책을 수립·운용하는 등 신용정보의 보호 및 관리에 대한 조치를 하여야 하며,

금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문 및 전자금융업무 등에 대한 보안대책 기준을 준수하여야 하는데도,

롯데카드㈜는 2023.1.1.~2025.8.28. 기간 중 온라인 결제 시스템을 운영하면서 다음과 같이 신용정보전산시스템에 대한 보안대책을 적정하게 수립·

운영하지 아니하고, 금융거래의 안전성과 신뢰성 확보를 위한 정보기술부문 및 전자금융업무 등에 대한 보안대책 기준을 준수하지 아니함으로써 2025.8.13.~2025.8.28. 기간 중 신원미상의 해커에 의해 롯데카드 고객 297만명의 신용정보가 유출되는 결과를 초래하였다.

(1) 정보처리시스템의 보정(patch) 작업 미실시*

* 「여신전문금융업법」 제54조의4, 「여신전문금융업감독규정」 제26조의4, 「전자금융감독규정」 제14조 등 위반

롯데카드는 전체 웹 어플리케이션 서버(총 20식) 중 일부에만 보안패치를 적용하고 온라인 결제 서버(5식)에는 중요 취약점 보안 패치의 보정작업을 미실시 하였다(정보유출 종료일인 2025.8.28. 기준).

서버 소프트웨어 제조사(오라클 社)는 해킹 위험에 따른 중요 보안 취약점 보안패치를 배포*하고, 금융보안원이 세 차례에 걸쳐 동 보안패치의 보정작업을 권고**하였으며, 금융감독원은 관련한 개선요구***를 한 바 있다.

* 2017.10월 오라클社가 중요 보안 취약점(CVE-2017-10271) 패치 배포

** 2018.1.11.~2024.10.11. 기간 중 금융보안원은 웹 어플리케이션 서버 프로그램(웹로직) 취약점에 대해 보안패치를 적용하라고 권고문을 3차례 전 금융회사에 발송

*** 2022.6.9.~7.8. 기간 중 실시된 금융감독원의 정기검사 결과 취약점 분석·평가 관리체계 관련 업무절차 등을 개선하고, 신규 취약점을 악용한 해킹 및 악성코드 감염 우려가 있는 기술지원이 종료된 전산자원을 업그레이드·교체하는 등 관리를 강화하도록 조치

(2) 침입차단·침입탐지시스템 미설치*

* 「여신전문금융업법」 제54조의4, 제54조의5, 「여신전문금융업법 시행령」 제19조의24, 「신용정보법」 제19조, 「신용정보법 시행령」 제16조 및 「신용정보업감독규정」 제20조, 별표 3 (II.1. 접근통제), 「전자금융감독규정」 제15조 등 위반

롯데카드는 정보보호장비인 웹방화벽에 해외카드 온라인 결제 웹서비스의 등록*을 누락함으로써 동 서비스에 침입차단 및 탐지시스템이 미설치되었다.

* 해킹 등 침해행위는 탐지 관문이 되는 웹 방화벽에 탐지 대상 서비스의 환경정보(웹서비스 IP주소, 서비스 포트 번호, 정보보안 서버정보 등)를 등록해야 해당 서비스의 선제적 침입탐지·차단 기능 수행 가능

(3) 주민등록번호 및 비밀번호 암호화 미이행*

* 「여신전문금융업법」 제54조의5, 「여신전문금융업법 시행령」 제19조의24, 「신용정보법」 제19조, 「신용정보법 시행령」 제16조 및 「신용정보업감독규정」 제20조, 별표 3(II.3. 개인신용정보의 암호화) 등 위반

롯데카드는 온라인결제시스템(내부망)에 비밀번호, 주민등록번호(개인식별번호) 등이 포함된 거래 기록(로그)를 저장하면서도 이를 암호화*하지 않았다.

* 저장과 동시에 암호화하지 않고 일정 시간(24시간~48시간)이 경과한 후 암호화되도록 운영함으로써 거래기록이 장시간 평문상태로 유지되도록 방치하였고, 비밀번호 네자리를 암호화하여 저장하지 않은 로그 파일 172,166건도 존재(다만, 이번 사고로 유출되지는 않았음)

(4) 바이러스 백신 소프트웨어 미설치*

* 「여신전문금융업법」 제54조의5, 「여신전문금융업법 시행령」 제19조의24, 「신용정보법」 제19조, 「신용정보법 시행령」 제16조 및 「신용정보업감독규정」 제20조, 별표 3(II.4. 컴퓨터바이러스 방지) 등 위반

롯데카드는 온라인 결제 웹 어플리케이션 서버(유닉스·리눅스)에 악성프로그램(웹쉘)이 설치되는 것을 선제적으로 탐지·차단·치료하기 위한 바이러스 백신 소프트웨어를 미설치* 하였다.

* 침해사고가 발생한 이후 해당 서버(유닉스·리눅스)에 백신 소프트웨어를 설치하자 동 백신 소프트웨어가 악성프로그램을 탐지하여 삭제하였음

※ 2025.6.20. 롯데카드 정보보호최고책임자(CISO)는 운영 리스크 미팅시 SK텔레콤이 리눅스 서버에 바이러스백신 등 보안 프로그램을 운영하지 않아 해킹사고 방지에 실패하였고, 롯데카드도 동일한 상황이라는 것을 대표이사 등 경영진에 보고하였음에도 별다른 보완 조치가 이루어지지 않음

(5) 신용정보보호 관련 법규 준수 여부에 대한 점검 소홀*

* 「여신전문금융업법」 제54조의5, 「여신전문금융업법 시행령」 제19조의24, 「신용정보법」 제19조, 「신용정보법 시행령」 제16조 및 「신용정보업감독규정」 제20조, 별표 3(III.1. 신용정보관리보호인) 등 위반

롯데카드의 신용정보관리·보호인은 2023년부터 2025년까지 “신용정보관리 및 보호 실태(금융분야 정보보호 상시평가)”를 점검하면서 대량의 개인신용

정보가 저장된 온라인결제시스템의 기술적·물리적·관리적 보안대책 적정성에 대해서는 점검하지 않았다.

그럼에도 불구하고, 롯데카드의 신용정보관리·보호인은 모든 신용정보전산시스템의 기술적·물리적·관리적 보안대책 점수를 100점으로 평가하여 대표이사 및 이사회에 이상이 없는 것으로 보고하였다.