금융위원회

의결 제2026-375호

1. 조치대상자의 인적사항

제재대상	내용(회사명, 성명 등)
기 관	롯데카드㈜
임 원	-
직 원	-

2. 조치내용

○ **(금감원 원안)** 「여신전문금융업법」에 따른 안전성 확보의무 및 신용정보 보호의무 위반에 대하여 업무 일부정지 4.5개월을 부과하고, 「신용정보법」에 따라 신용정보 보호의무 위반에 따른 개인신용정보 유출에 대하여 과징금 50억원 부과 조치

○ **(수정의결)** 금감원 원안을 일부 수정하여 업무 일부정지 1.5개월을 부과

제재대상	기관제재	
	원안	수정안
롯데카드㈜	업무 일부정지 4.5개월 부과	업무 일부정지 1.5개월 부과

○ **(수정의결 사유)** 법 위반의 정도, 기존 제재사례와의 형평성, 사후 수습 노력 등을 종합적으로 감안하여 업무정지 기간을 1.5개월로 재산정

3. 조치이유

가. 지적사항

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

○ **(금감원 원안)** 「여신전문금융업법」 제54조의4 및 제54조의5, 「신용정보의 보호 및 관리에 관한 법률」 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,

- 롯데카드는 20xx.x.x.~20xx.x.xx. 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 20xx.x.xx.~20xx.x.xx. 기간 중 신원미상의 해커에 의해 롯데카드 고객 xxx만명의 신용정보가 유출되는 결과를 초래하였음

(1) 정보처리시스템의 보정(patch) 작업 미실시

○ **(금감원 원안)**「여신전문금융업법」제54조의4, 「전자금융감독규정」 제14조 등에 의하면, 신용카드업자는 정보처리시스템의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정작업을 하여야 하며, 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호 시스템을 설치 및 운영하여야 함에도

- 롯데카드는 전체 웹 어플리케이션 서버(총 xx식) 중 일부에만 보안 패치를 적용하고 온라인결제 서버(x식)에는 중요 취약점 보안 패치의 보정작업을 미실시 하였음

(2) 침입차단·침입탐지시스템 미설치

○ **(금감원 원안)**「여신전문금융업법」제54조의5, 「신용정보업 감독규정」 제20조 등에 의하면, 신용카드업자는 개인신용정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하여 보호해야 함에도

- 롯데카드는 정보보호장비인 웹방화벽에 해외카드 온라인 결제 웹서비스의 등록을 누락함으로써 동 서비스에 침입차단 및 탐지 시스템이 미설치되었음

(3) 주민등록번호 및 비밀번호 암호화 미이행

○ **(금감원 원안)**「여신전문금융업법」제54조의5, 「신용정보업 감독규정」 제20조 등에 의하면, 신용카드업자는 비밀번호, 생체인식정보 등 본인임을 인증하는 정보는 암호화하여 저장하며, 이는 조회할 수 없도록 하여야 함에도

- 롯데카드는 온라인결제시스템(내부망)에 비밀번호, 주민등록번호(개인식별번호) 등이 포함된 거래 기록(로그)를 저장하면서도 이를 암호화하지 않았음

(4) 바이러스 백신 소프트웨어 미설치

○ **(금감원 원안)** 「여신전문금융업법」 제54조의5, 「신용정보업 감독규정」 제20조 등에 의하면, 신용카드업자는 정보처리기기에 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 함에도

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

(5) 신용정보보호 관련 법규 준수 여부에 대한 점검 소홀

○ **(금감원 원안)** 「여신전문금융업법」 제54조의5, 「신용정보업 감독규정」 제20조 등에 의하면, 신용정보관리·보호인은 임직원 등의 신용정보보호 관련 법령 및 규정 준수 여부를 점검하여 경영진에 보고하여야 함에도

- 롯데카드의 신용정보관리·보호인은 20xx년부터 20xx년까지 “신용정보 관리 및 보호 실태(금융분야 정보보호 상시평가)”를 점검하면서 대량의 개인신용정보가 저장된 온라인결제시스템의 기술적·물리적·관리적 보안대책 적정성에 대해서는 점검하지 않았음

나. 근거법규

○ 「여신전문금융업법」 제54조의4 제2항, 제54조의5 제1항 및 제4항, 제57조 제1항 제2호
○ 「여신전문금융업법 시행령」 제19조의24 제1항, 제21조 제1항 및 제2항
○ 「신용정보의 이용 및 보호에 관한 법률」 제19조 제1항, 제20조 제3항, 제4항 및 제6항, 제42조의2 제1항 제1호
○ 「신용정보의 이용 및 보호에 관한 법률 시행령」 제2조 제6항, 제16조 제1항, 제2항, 제17조 제7항 및 제8항

○ 「신용정보업감독규정」 제20조, [별표3]

○ 「전자금융감독규정」 제14조 제4호, 제15조 제1항 제1호