금융위원회

의결 제2026-1호

1. 조치대상자의 인적사항

제재대상	내용(회사명, 성명 등)
기 관	모아저축은행㈜

2. 조치내용

□ 기관에 대한 조치

◦ 「신용정보의 이용 및 보호에 관한 법률」상 신용정보전산시스템의 안전보호의무 위반에 대하여 과징금 12억 4,300만원 및 「전자금융거래법」 상전자금융거래의 안전성 확보의무 위반에 대하여 과태료 1억 4,000만원 부과

3. 조치이유

가. 지적사항

□ 기 관

1. 신용정보전산시스템의 안전보호의무 위반

□ 「신용정보법」 제19조 제1항, 동법 시행령 제16조에 의하면, 신용정보제공·이용자는 신용정보전산시스템의 안전보호를 위해 「신용정보업감독규정」 제20조 [별표 3]에 정한 기술적·물리적·관리적 보안대책을 수립·시행하여야 함에 따라

신용정보제공·이용자는 ①취급 중인 개인신용정보가 인터넷 홈페이지 등을 통하여 열람 권한이 없는 자에게 공개되지 않도록 하여야 하고 ②신용정보관리·보호인을 통하여 개인신용정보 처리 실태 등에 대한 정기적인 조사·개선을 실시하여야 하는데도,

① 모아저축은행은 공개용 웹서버에 개인신용정보를 조회할 수 있는 프로그램을 등록(20xx. xx. xx.)하고 적절한 통제수단 없이 열람 권한이 없는 자에게 개인신용정보가 공개*될 수 있도록 하였으며,

* 관리자 아이디·비밀번호 입력 또는 IP주소 등 접근통제 없이 간단한 명령어(쿼리) 입력만으로 개인신용정보 조회 가능한 상태

② 동 저축은행 신용정보관리·보호인은 대량의 정보가 유출될 수 있는 모아론(대출) 홈페이지 등 공개용 웹서버에 대하여 개인신용정보 처리 실태 및 관행에 대한 정기적인 조사·개선을 실시하지 않았음

○ 이로 인해, 모아저축은행은 모아론(대출) 홈페이지 등이 해킹공격에 취약한 상태로 운영된 사실을 장기간(xx년 xx일, 20xx.xx.xx.~20xx.xx.xx.) 인지하지 못하고 방치하였으며,

○ 그 결과, 20xx. xx. xx. ~ 20xx. xx. xx. 기간 중 해킹공격으로 인해 전체 ●명의 개인정보(●명) 및 개인신용정보(●명)가 유출되었음

2. 전자금융거래의 안전성 확보의무 위반

(1) 해킹 등 방지대책 운용 의무 위반

□ 「전자금융거래법」 제21조 제2항, (舊)「전자금융감독규정」 제7조 제3호, 제15조 제2항 제3호, 제4항에 의하면, 금융회사는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 ① 정보보호시스템을 설치·운영하는 경우에는 보안정책의 승인·적용 및 등록·변경·삭제에 대한 이력을 기록·보관하고, ② 해킹 등으로 인한 피해 발생

시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 하는데도,

① 모아저축은행은 검사종료일(2024.3.15.) 현재 정보보호시스템 ●종을 설치·운영하면서 네트워크 접근관리시스템 등 2종은 최초 도입 시부터, 방화벽 등 나머지 ●종은 최대 ●년 ●개월간 보안정책 관련 이력을 기록·보관하지 않았고

② 해킹행위 및 이로 인한 피해가 탐지되는 경우 담당자에게 알람 메시지로 즉시 통보하여 신속히 조치할 수 있는 대응체계를 마련하지 않았음

○ 이로 인해, 20xx. xx. xx. ~ 20xx. xx. xx. 해킹공격을 당했는데도 담당자에게 피해사실이 즉시 통보되지 않아 신속한 조치가 이루어지지 않았음

(2) 홈페이지 등 공개용 웹서버 관리대책 수립·운용 의무 위반

□ 「전자금융거래법」 제21조 제2항, (舊)「전자금융감독규정」 제7조 제3호, 제17조 제4항에 의하면, 금융회사는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 하는데도,

○ 모아저축은행은 20xx. xx. xx. ~ 20xx. xx. xx. 기간 중 모아론(대출) 홈페이지 등 공개용 웹서버에 대한 해킹공격을 방지하기 위해 방화벽을 운용하면서 해킹공격이 즉시 차단되지 않고 모니터링(탐지)만 되도록 방화벽을 미흡하게 설정하였음

○ 이로 인해, 해커가 공개용 웹서버의 개발용 프로그램을 통해 고객정보를 탈취하였는데도 이를 즉시 차단하지 못하였음

(3) 프로그램 등록 절차 수립·운용 의무 위반

□ 「전자금융거래법」 제21조 제2항, (舊)「전자금융감독규정」 제7조 제3호, 제29조 제3호 및 제7호에 의하면 금융회사는 프로그램을 운영시스템에 등록 시 ① 그 정당성에 대해 제3자의 검증을 받아야 하고, ② 전산자료 관리자 등 해당 프로그램 담당자 이외의 자가 등록을 수행하여야 하나,

모아저축은행은 20xx.xx.xx.~20xx.xx.xx. 기간 중 모아론(대출) 홈페이지 등 신규 서비스*를 위한 정보화사업을 추진하면서,

* 대출 신청·접수 홈페이지 및 ○○○○○ 연계 대출 서비스

① 동 프로그램 목록·수량·등록내용의 이상 유무 등 정당성에 대해 제3자 검증을 누락하였고,

② 해당 개발자가 관련 프로그램을 운영시스템에 직접 등록(20xx. xx. xx.)하도록 하여 외부망에 위치한 공개용 웹서버에 설치되어서는 안 되는 개인신용정보가 저장된 데이터베이스 접근·조회가 가능한 개발용 프로그램까지 운영시스템에 등록되었음

(4) 암호키 관리 통제 의무 위반

□ 「전자금융거래법」 제21조 제2항, (舊)「전자금융감독규정」 제7조 제3호, 제31조 제2항에 의하면 금융회사는 암호 및 인증시스템에 적용되는 키(이하, '암호키')에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 하는데도,

○ 모아저축은행은 타 금융회사와의 전문 송·수신 등에 사용하는 암호키 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하지 하지 않고 미흡하게 관리하여 20xx. xx. xx. ~ 20xx. xx. xx. 기간 중 해커에 의해 암호키가 유출되었음

(5) 비밀번호 관리 의무 위반

□ 「전자금융거래법」 제21조 제2항, (舊)「전자금융감독규정」 제7조 제3호, 제32조 제2호 나목에 의하면 금융회사는 내부사용자 비밀번호는 유출을 방지하기 위하여 보관 시 암호화하여야 하는데도,

○ 모아저축은행은 비밀번호(●개)를 암호화하지 않고 관련 파일·프로그램에 평문으로 보관·사용하도록 미흡하게 관리하여 20xx. xx. xx. ~ 20xx. xx. xx. 기간 중 해커에 의해 비밀번호가 유출되었음.

나. 근거법규

□ 기관에 대한 조치

<신용정보법>

1. 「신용정보의 이용 및 보호에 관한 법률」 제19조 제1항
2. 「신용정보의 이용 및 보호에 관한 법률」 제42조의2 제1항
3. 「신용정보의 이용 및 보호에 관한 법률 시행령」 제16조
4. 「신용정보업감독규정」 제20조 [별표 3]

<전자금융거래법>

1. 「전자금융거래법」 제21조 제2항
2. 「전자금융거래법」 제51조 제1항
3. (舊)「전자금융감독규정」 제7조 제3호
4. (舊)「전자금융감독규정」 제15조 제2항 제3호, 제4항
5. (舊)「전자금융감독규정」 제17조 제4항
6. (舊)「전자금융감독규정」 제29조 제3호, 제7호
7. (舊)「전자금융감독규정」 제31조 제2항
8. (舊)「전자금융감독규정」 제32조 제2호 나목