경영유의사항 등 공개안

1. 금융회사명 : 신한카드㈜

2. 조치일 : 2023. 12. 21.

3. 조치내용

대상	내 용
기관	경영유의 2건, 개선 4건

4. 조치대상사실

가. 경영유의사항

⑴ 부정사용예방시스템 운영 및 관리 강화

신용카드 부정사용예방시스템(Fraud Detection System, 이하 'FDS')에서 앱카드를 통한 일부 연속적 거래에 대하여 이상거래 경보(alert)가 수차례 발령되더라도 금액적 중요성이 낮다는 이유 등으로 카드회원에 대한 전화통화, 거래정지 등 별도의 대응 없이 전부 정상거래로 처리하고 있으며

카드 이상거래를 회원이 보유한 전체 신용카드가 아닌 신용카드별 사용내역으로 판단하고 사용정지 등의 조치를 취하고 있어, 복수 신용카드를 보유한 회원의 경우 일부 신용카드에서 부정사용이 이루어지더라도 회원이 보유한 전체 신용카드가 아닌 일부 신용카드에 대해서만 사용정지를 하는 등 신용카드 부정사용 피해 예방에 적극적으로 대처하지 못하였으므로

앞으로, 연속적 거래와 관련된 이상거래의 경보 및 대응 체계를 개선하는 한편, 현행 카드 단위의 모니터링 체계를 회원 단위로 변경하는 등 FDS 운영 및 관리를 강화할 필요가 있음

⑵ 모바일 앱카드에 대한 부정사용 예방 활동 강화

이용자가 단말기에 모바일 앱카드('신한pLay')를 설치하는 경우 이용자 단말기의 이상징후(루팅*, 원격제어 등)를 탐지하는 기능도 함께 운용하고 있으나,

* 안드로이드 운영체제를 탑재한 모바일 기기에서 관리자 권한을 획득하는 행위

카드 부정사용 등의 사고를 방지하기 위하여 이용자 단말기에서 수집한 이상징후 탐지정보*를 분석하는 사고 예방 체계**가 미흡하여 이용자 단말기의 취약점을 이용한 모바일 앱 카드 관련 사고가 지속 발생할 우려가 있으므로

* 이상징후 패턴(루팅 등), 탐지일시, 단말기 IP주소, 운영체제(OS), 앱 버전 및 앱 설치 아이디 등
** 사고 단말기 거래 제한, 해킹 등 공격자 의심 블랙리스트 IP 거래 차단, 멀티 휴대폰 로그인 거래 검증 등

이용자 단말기에서 수집한 이상징후 탐지정보를 활용한 사고예방 기준과 절차를 마련·운용하고, 사고 개연성이 높은 거래*에 대해서는 FDS시스템 및 정보보호시스템 등과 연계하는 등 모바일 앱 카드에 대한 사고 예방 활동을 강화할 필요가 있음

* 과거 부정사용에 이용된 특정 IP를 통한 다수 회원 명의의 연속적인 온라인 부정거래 등

나. 개선사항

⑴ 카드 부정사용 재발 방지를 위한 업무절차 미흡

내규「Fraud 리스크 관리 지침」에 의하면 정보유출로 추정되는 회원에 대한 적절한 조치를 통해 사고를 예방하고 회사 및 회원의 손실을 최소화하여야 하는데도

2022.4월 중 고객센터에 유사한 유형의 신용카드 부정사용 민원이 다수 접수되었으나, FD팀 등 유관부서가 부정사용 민원으로 인지하지 못하거나*, 부정사용 민원으로 인지하였더라도 신속한 사고조사 및 재발 방지를 위한 후속 대응 등이 미흡하여 카드 부정사용을 조기에 차단하지 못하였으므로

* 고객센터에서 부정사용 민원을 일반민원으로 코드를 부여함에 따라 FD팀에서 해당 민원을 부정사용 민원으로 미인지

앞으로 부정사용 민원을 적시에 인지하여 대응할 수 있도록 전산 시스템을 마련하는 한편 부정사용 민원이 발생하는 경우에는 FD팀 사고조사 담당자를 배정하여 신속히 대응하도록 하는 등 카드 부정사용 민원의 조기 인지 및 재발 방지와 관련된 업무절차를 개선하시기 바람

⑵ 모바일 앱 고객 통지대책 미흡

동일한 이용자가 복수의 단말기에 모바일 앱을 설치·이용할 수 있도록 멀티 디바이스 정책을 운용하고 있으나,

불상자가 피싱 등의 방법으로 수집한 고객정보*를 도용하여 이용자가 소유하지 않은 불상의 단말기에 모바일 앱을 설치하고 카드를 부정 사용할 가능성이 있음에도 타 단말기의 로그인 정보에 대한 고객 통지 절차가 없고,

* 성명, 휴대폰번호, 카드번호, CVC, 카드비밀번호

모바일 앱 알림서비스*의 경우 동 앱이 마지막에 설치된 단말기에 한정하여 알림서비스를 운영하고 있어 고객이 카드부정사용 사실을 인지하지 못해 고객 피해가 지속적으로 발생할 가능성이 있으므로

* 카드 결제·승인내역, 부가정보 등을 모바일 앱에 장착된 알림메시지 기능을 통해 제공하는 서비스로 별도의 이용수수료는 부과하지 않음

고객이 모바일 앱에 접속하는 경우 타 단말기에서의 로그인 정보를 통지하는 등 고객이 카드부정사용 사실을 조기에 인지할 수 있도록 모바일 앱 고객 통지대책을 개선하시기 바람

⑶ 모바일 앱 버전 관리 미흡

모바일 앱 보정(Patch)을 위한 업무협의체를 구성하여 정기적인 보정작업을 통해 모바일 앱의 보안취약점 및 버전을 관리하고 있으나,

기술지원이 중단(EOS)되어 신규 보안취약점에 대한 보정이 불가한 모바일 단말기 운영체제(OS)에 대해서도 모바일 앱 설치를 허용하고 있고, 2020.2.19.부터 검사착수일(2022.5.2.)까지 출시된 “신한pLay” 모바일 앱 버전 전체(34개)에 대해서도 최신 버전 업데이트 유도 없이 이용자 접속을 전부 허용하고 있어 모바일 앱 이용자가 적시에 보안업데이트를 수행하지 못하는 등 보안취약점에 노출될 우려가 있으므로

문자 등 고객 통지수단을 통해 지속적으로 모바일 앱 업데이트를 유도하고, 단말기 운영체제(OS) 버전 안전성 등을 고려하여 과거 버전 접속을 점진적으로 차단하는 등 모바일 앱 버전에 대한 관리 절차를 개선하시기 바람

(4) 모바일 앱 이용자 인증수단 관리 미흡

모바일 앱('신한pLay') 가입을 위해 스마트간편인증, ARS인증, SMS인증 등 다양한 인증방법을 적용하여 운영 중이나,

신한pLay 가입을 위한 Outbound ARS 인증*시 인증결과를 서버에서 확인하지 아니하고 앱에서만 확인하고 있어 인증결과 변조**를 통해 ARS인증을 우회할 수 있으며,

* 신한카드㈜에서 이용자에게 전화를 걸어 이용자가 화면에 보이는 인증코드를 입력하는 방식
** 휴대폰에서 ARS인증시 인증 성공여부와 관계없이 앱에서 인증결과를 임의로 변조(실패→성공)

휴대폰 SMS인증의 경우 인증오류 횟수를 제한하지 않고 있어 타인이 인증번호 전수입력 툴 등을 통해 고객 본인인증을 우회할 가능성이 있으므로

모바일 앱에 적용된 인증 관련 프로그램 전반에 대하여 인증결과값 변조 등의 인증 우회 가능성을 점검하고, 휴대폰 SMS 인증번호 오류횟수를 제한하는 등 모바일 앱 이용자 인증수단에 대한 관리 절차를 개선하시기 바람