경영유의사항 등 공개안

1. 금융기관명 : 나이스페이먼츠㈜

2. 조치일 : 2019. 10. 2.

3. 조치내용

대상	내용
기 관	개선사항 6건

4. 조치대상사실

가. 경영유의사항

(1) 약관 내 배상 책임 및 면책 범위 불합리

「전자금융거래 이용약관」 제10조에 회사의 전자금융사고에 대한 손해배상 책임 및 면책 사유 등을 규정하고 있으나,

사고 발생에 있어서 '이용자의 고의나 중대한 과실이 있는 경우'로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다*는 취지의 회사 면책에 대한 '전제조건'이 약관에 명시되어 있지 않아 실무적으로는 회사가 이용자의 '고의 및 중과실' 여부를 증명하지 않고 배상 책임을 이용자에게 전가하게 될 여지가 있고,

* 「전자금융거래법」 제9조(전자금융업자의 책임)제2항 및 동 시행령 제8조(고의나 중대한 과실의 범위)

법령에 규정된 면책 사유에 해당하지 않는 사유(천재지변, 회사의 귀책사유가 없는 정전 등)로 손해배상 책임을 면하도록하여 이용자에게 불리한 조항이 있어 배상 책임 및 면책 범위와 관련한 분쟁이 발생할 가능성이 있으므로

이용자에게 불리한 조항이 발생하지 않도록 회사의 배상 책임 및 면책 범위를 법령상의 기준으로 조정하여 「전자금융거래 이용약관」에 명시함으로써 이용자의 혼동 및 불필요한 분쟁 등을 예방할 필요

(2) 결제 예치대금 정산관리 불합리

결제예치대금(Escrow)에 대한 정산 처리를 위해 결제 후 2주일 이상 배송정보를 등록하지 않음으로 인해 정산 처리가 완료되지 않은 가맹점에 대해서 주 1회 이메일로 관련 내용을 안내하고 있으나,

담당자 변경에 따른 안내 메일 미수신 등의 사유로 미정산 금액을 인지하지 못함으로써 검사착수일 현재 OOOO개의 가맹점에서 결제 예치대금 잔액(총 OO억원)이 결제 후 2주일 이상 미정산 상태로 남아있고, 이중 O천만원 이상 고액의 미정산 금액이 남아있는 가맹점은 OO개(총 OO억원)로 전체 미정산 금액의 OO%에 해당하는 등 장기 미정산으로 인해 가맹점의 금전적 피해가 발생할 우려가 있으므로

고액의 결제 예치대금이 장기간 미정산 상태로 남겨지지 않도록 가맹점 관리시스템 접속 시 동 미정산 내용에 대하여 팝업으로 안내하거나, 휴대폰 문자메시지(SMS) 등을 통해 알림으로써 결제 예치대금이 원활하게 정산될 수 있도록 하는 등 관련 업무 절차를 보완하여 가맹점 정산에 대한 관리를 개선할 필요

(3) 원격접속 통제·관리 불합리

야간 또는 공휴일에 긴급한 장애처리 등을 위해 외부에서 내부시스템 접속 시 가상사설망(VPN)을 이용하고 원격PC는 동 내부시스템 연결 이외의 다른 인터넷 연결은 차단하도록 설정하고 있으며, 백신 및 윈도우 업데이트 최신 여부를 점검하는 등 원격접속 통제 절차를 운영하고 있으나,

원격접속 이용에 대한 유효기간을 설정하지 않아 사용자가 원격접속을 위해 최초 승인받은 이후 별도 책임자 승인 없이 원격접속 권한을 유지할 수 있고, 원격접속을 통해 수행한 작업 내역에 대해서는 그 적정성을 사후 확인하지 않아 인가된 업무 목적 이외의 원격 접속시도가 발생할 우려가 있으므로

보안리스크를 고려하여 원격접속 이용에 대한 유효기간을 설정하는 한편, 원격접속 작업 내역에 대한 적정성을 사후 점검할 수 있도록 관리 방안을 개선할 필요

(4) 취약점 분석·평가 관리 불합리

전자금융 기반시설의 취약점 분석·평가를 연 1회 이상(홈페이지는 6개월에 1회 이상) 실시하고 발견된 취약점에 대해서는 이행계획을 수립하여 조치하고 있으나,

취약점 점검 및 이행진단을 수행하는 전담 인력이 없어 일부 취약점 진단 결과에 대한 이행점검이 미흡하였고, 취약점 이행 조치를 조기에 실시하지 않거나 적절히 조치하지 않아 장기간 다수의 취약점이 잔존하고 있으며, 매년 동일한 취약점이 반복하여 발견되는 등 취약점 관리가 미흡하므로

취약점 점검 및 이행점검 관리를 체계적으로 수행하도록 전담 인력을 지정하여 취약점 이행점검 현황을 자체적으로 점검하는 등 취약점 관리 절차를 수립하는 한편, 동일한 취약점이 반복되지 않도록 프로그램 개발 인력을 대상으로 취약점 조치 방법 등에 대한 교육을 실시하는 등 취약점 분석·평가 관리를 개선할 필요

(5) 전산자료의 백업·소산 관리 불합리

장애, 재해 등 비상사태에 대비하여 전자금융거래 관련 데이터베이스(DB), 거래로그 등 주요 전산자료를 정기적으로 백업하고, DB 백업자료는 소산장소(OOO 위치)에 보관하고 있으나,

일부 정보처리시스템(DB서버 등)의 운영체제(OS) 및 설정파일, 프로그램 파일 등의 전산자료에 대해서는 백업을 실시하지 않고, 데이터베이스(DB) 파일 이외 백업 자료는 원격지 소산 대상에 포함하지 아니하여 전산센터 재해 발생 시 정보처리 시스템에 대한 신속한 복구가 어려울 우려가 있으므로

DB서버의 운영체제 등에 대해서도 백업을 확대하여 실시하고, 전산센터 재해에 대비하여 전자금융 거래로그, 설정파일 등의 백업자료도 소산대상으로 포함하여 관리하는 등 백업·소산 관리를 개선할 필요

(6) 업무지속성 확보대책 불합리

비상상황 시 업무지속성을 확보하기 위해 내규「사고대응지침」및「백업 및 복구 관리절차」를 마련하고 동 지침에 따라 연 1회 비상대응훈련을 실시하고 있으나,

2016년~2018년 기간 중 실시한 비상대응훈련은 전산센터 정전 상황만을 가정하여 실시(매년)한 반면, 전자금융업무(전자지급결제대행, 결제대금예치) 중단 등 다양한 시나리오를 기반으로 한 비상대응훈련을 실시하지 않아 동 훈련을 통한 업무지속성 확보대책의 실효성을 검증하기 어렵고

실제 비상상황 발생을 대비한 복구시스템 및 인프라 구성현황, 복구시스템 가동·복원 절차 등을 포함한 상세 업무매뉴얼을 마련하지 않아 다양한 긴급 상황을 대비한 대응체계가 미흡하여 업무지속성 확보에 어려움이 예상되므로

전자금융업무 중단 등 다양한 비상상황에 대비한 훈련 시나리오 기반의 훈련을 실시하여 비상대응훈련의 실효성을 확보하고, 비상상황 시 시스템 복구를 위한 상세 복구절차 등이 포함된 업무매뉴얼을 마련하여 업무지속성 확보대책을 개선할 필요