경영유의사항 등 공개안

1. 금융기관명 : ㈜카카오페이

2. 조치일 : 2021. 5. 3.

3. 조치내용

대상	내용
기 관	경영유의사항 3건, 개선사항 13건

4. 조치대상사실

가. 경영유의사항

(1) 전자금융 및 IT부문 업무 내부통제 강화

회사는 '선불전자지급수단 발행 및 관리업' 및 '전자지급결제대행업(PG)' 등 전자금융업을 영위하고 있으나,

전자금융 및 관련 IT부문 업무에 대한 적정성, 준법성을 주기적으로 점검하는 감사조직 및 규정이 없고 준법감시·감사기능 등 내부통제 체계가 적정하게 구축되지 않아 전자금융 및 IT부문 업무에 미흡사항*이 발견되고 있으므로

* 클라우드 이용, 망분리 이행, 공개용 웹서버 관리, 프로그램·전산원장 통제, 약관 변경관리, 취약점 분석·평가 관리, 전산자료 반출통제, 자체보안성심의, 장애관리 등

앞으로 전자금융 및 IT업무에 대한 적정성, 준법성을 주기적으로 점검할 수 있도록 준법감시 기능을 강화하고, 감사 기능(IT포함)을 신설하는 등 내부통제 체계를 강화할 필요가 있음

(2) 경영건전성 유지방안 수립·이행 강화

회사는 OOOO.O월말 현재 자기자본 OOOO억원, 미상환잔액 대비 자기자본 비율 OO%, 유동성 비율 OO%로 경영지도기준을 충족하고 있으나,

OOOO.O월말 및 OOOO.O월말 기준 미상환잔액 대비 자기자본 비율이 각각 OO%로 경영지도기준(20% 이상)을 충족하지 못하였고, 특히 OOOO.O월말 기준 업무보고서 제출시(OOOO.O.O)에는 내부회계시스템을 통해 미상환잔액 대비 자기자본 비율이 충족하지 못하는 상황임을 사전에 인지할 수 있었음에도 이를 확인하지 않은 채 O월말 기준으로 오작성하여 미상환잔액 대비 자기자본 비율을 충족(OO%) 상태로 보고한 사실이 있음

또한, OOOO년 당기순손실이 △OOO억원에 달하는 등 매월 적자가 지속적으로 발생하고 있어 미상환잔액 대비 자기자본 비율이 충족하지 못할 우려가 있음에도 경영진에 이와 같은 사실을 보고하지 않는 등 리스크 관리가 미흡하므로

앞으로 경영지도기준 준수 여부를 주기적으로 확인할 수 있도록 내부 모니터링 절차를 마련하고 그 결과를 경영진에 보고하는 한편, 경영지도기준을 충족하지 못할 상황이 발생할 경우 상세한 경영개선계획(투자 유치계획 등)을 마련하여 주기적으로 이행실적을 점검하는 등 경영건전성 유지 방안 수립·이행을 강화할 필요가 있음

(3) 미환급 선불충전금 잔액 이용자 환급이행 강화

선불전자지급수단을 통해 간편송금, 간편결제 등 다양한 전자금융서비스를 제공하고 있으나,

OOOO.O.O. ~ OOOO.O.O. 기간 동안 이용자에게 환급하지 않은 선불충전금 잔액(총 OO억원)을 보유하고 있음에도 해당 이용자에게 미환급 선불충전금 잔액을 환급해주기 위한 별도 안내절차 및 세부 환급절차를 마련하지 않아

이용자가 본인 소유의 선불충전금 잔액 여부를 정확히 인지하지 못하여 금전 피해가 발생할 우려가 있으므로

앞으로 이용자에게 미환급 선불충전금 잔액에 대해 알림 채널(OOOO 알림메시지, SMS 등)을 통해 별도 안내하고, 본인확인 등을 통해 해당 이용자의 선불잔액을 조속히 환급할 수 있는 절차를 마련할 필요가 있음

나. 개선사항

(1) 전자금융거래 약관 통지 방법 및 통지내용 확인절차 개선

회사는 전자금융거래 약관을 변경 시 그 시행일 1월 전에 전자금융서비스에 가입된 모든 이용자에게 약관 변경사실을 통지하여야 하고, 이용자가 이의를 제기할 경우 이용자에게 적절한 방법으로 통지하였음을 확인해주어야 하나,

약관 변경 후, 이용자 중 OOOO OO서비스의 'OOOOO'를 친구로 등록한 이용자에게만 통지하거나 OOO 앱을 삭제 또는 서비스를 탈퇴한 이용자에게 통지를 누락하는 등 OOO 앱 미이용 고객에 대해서는 약관 변경 통지를 하지 않고 이의 제기에 따른 통지 확인 절차를 제공하지 않고 있으므로,

앞으로 OOOO을 사용하지 않는 이용자에 대해서도 약관 변경에 따른 사전 통지 및 통지내용 확인이 이루어질 수 있도록, 휴대폰 SMS, 전자메일 등으로 통지방법을 다양화하는 등 관련 절차를 개선하시기 바람

(2) 자체 보안성심의 실시 판단기준 및 운영절차 개선

① 신규 전자금융업무를 수행하거나 제휴서비스를 제공하는 경우 자체 보안성심의를 진행하고 있으나,

자체 보안성심의를 전자금융 서비스 개시 이후에 실시하는 등 안전성이 확보되지 않은 상태에서 서비스를 제공하는 사례가 확인되고 있으므로

앞으로 자체 보안성 심의 완료 후 서비스를 개시하도록 자체 보안성심의 운영·관리 절차를 개선할 필요가 있음

② 자체 보안성심의 내용을 내규 「OOOOOOOOO」에 일부 반영하고 있으나, 자체 보안성심의 실시 판단기준과 세부 운영절차를 별도로 마련하고 있지 않아 자체 보안성심의 실시 또는 금융감독원 보고가 누락될 우려가 있으므로

앞으로 자체 보안성심의 실시 판단기준과 세부 운영절차를 개선하여 내규에 반영하고, 자체 보안성심의 결과보고가 누락되거나 지연되지 않도록 자체 보안성심의에 대한 관리를 강화할 필요가 있음

(3) 취약점 분석·평가 관리 미흡

① 전자금융기반시설의 취약점 분석평가를 연 1회(홈페이지는 6개월에 1회 이상) 실시하고, 발견된 취약점에 대해서는 이행계획을 수립하여 조치를 시행하고 있으나

OOOO~OOOO년 취약점 분석·평가시 신규 도입 및 용도 변경된 서버에서 과거 조치 완료된 취약점과 동일한 유형의 취약점이 반복적으로 발견되고 있으므로

앞으로 업무담당자를 대상으로 과거에 발견된 취약점 및 조치방법 등에 대해 교육을 실시하여 관련 직원들이 이를 숙지토록 하는 등 동일 유형의 취약점이 반복적으로 발생하지 않도록 조치할 필요가 있음

② 자체 결제 방식을 사용하는 제휴사(OO, OO 등)에 회사의 결제수단을 제공하면서 동 결제서비스 관련 프로그램에 대한 취약점 분석·평가를 수행하였으나

제휴사 연관 전자금융거래 OOOO 및 OOOO OOOO OO, OOOO OOOO에 대한 기술적·관리적 취약점 분석·평가를 실시하지 않아 결제수단 등의 부정·도용 사고 대응이 미흡하므로

앞으로 제휴사와 연관된 전자금융거래 OOOO 및 OOOO OOOO OO, OOOO OOOO에 대한 기술적·관리적 취약점 분석평가를 실시하여 분실·도난·부정·도용 및 위·변조 사고예방을 위한 기술적 조치방안을 마련하고

사고발생시 이용자에 대한 제휴사 및 회사 간의 보상주체 명확화, 이용자 및 가맹점 주의사항 안내, 보호수단* 홍보 등 관리적 조치방안을 마련하여 시행할 필요가 있음

* 회사 및 제휴사에서 제공하는 잠금화면 설정, OTP사용 등

(4) 문서파일·전산자료 반출통제 미흡

① 이용자 정보를 처리하는 내부업무시스템의 안전한 운영을 위해 시스템 접속 및 단말기 매체 사용을 통제하고, 과다 반출자에 대한 소명절차를 마련하여 월 1회 점검을 실시하고 있으며

내부업무시스템에 수록된 고객정보의 외부 반출 시에는 OO OO OOOO OO, OOO OOOO OO, OOOOOOOO OOOO OO, OOOOOO 등 반출통제 장치를 이용하고 있으나

과다반출자에 대한 상시 모니터링을 수행하지 않고 있고, 내부업무시스템의 접속 화면에 대한 화면 캡처를 허용하고 있으며, 회사 단말기로 외부 장소에서 문서 출력시 출력이력을 남기지 않아 고객정보 등 전산자료 반출에 대한 통제가 미흡하므로

앞으로 고객정보, 회사 민감자료 등의 반출 시에는 고객정보의 검출건수와 상관없이 반출업무 담당자가 적정성을 검증하고 책임자의 사전 승인 후에만 반출하도록 하는 등 과다 반출자에 대한 상시 모니터링을 수행할 필요가 있으며

내부업무시스템에서 고객정보 조회 시 화면캡처 방지 기능 등을 적용하고, 회사 외부장소에서 문서 출력이 이루어지는지 모니터링하여 불가피하게 출력이 필요한 경우에는 통제 담당자가 적정성을 검증하고 책임자의 승인이후에만 출력토록 하는 등 내부업무시스템 및 프린터 사용에 대한 통제를 실시할 필요가 있음

② 업무상 필요로 인해 인터넷 단말기를 통하여 고객정보를 반출하는 경우, 업무목적 달성 이후 동 인터넷 단말기 내에 해당 파일을 삭제하였는지 여부를 확인하지 않고

인터넷 단말기 내 회사의 각종 문서파일에 대해서는 이메일, 메신저 등을 통한 반출 차단이 이루어지지 않는 등 통제가 미흡하므로

앞으로 인터넷 단말기에 저장된 이용자 정보는 해당 업무목적이 달성된 이후에는 즉시 삭제하도록 하고

인터넷 단말기를 통한 고객정보, 회사 중요문서 등의 유출방지를 위해 동 단말기에 대한 웹사이트 접속 및 프로그램 사용 통제를 강화하는 한편, 고객정보 파일, 회사 중요문서 등 전산자료에 대한 암호화 기능을 적용하는 등 보완대책을 마련할 필요가 있음

(5) 접근통제시스템 운영 미흡

① 시스템 접근권한 제어 등을 위하여 서버 접근통제시스템 및 데이터베이스(DB) 접근통제시스템을 도입하여 운영하고 있으나,

서버관리자가 서버(전산실, 클라우드) 접속 시 최고관리자 계정(root)으로 로그인하고 있어 작업자 실수 등으로 시스템 파일이 임의로 삭제될 위험이 있고,

DB관리자가 OOOO OOO 데이터베이스 관리 시스템(DBMS) 접속 시에는 DB접근통제시스템을 통하지 않고 로그인하고 있어 DB자료의 삭제·변경 등 주요 작업이 통제되지 않을 우려가 있으므로,

앞으로 서버관리자가 서버 운영체제 로그인시 최고관리자 계정(root)이 아닌 일반 사용자 계정으로만 접속하도록 하고 OOOO OOO DBMS 등에 대해서도 접근통제 시스템을 경유하여 접속하도록 운영할 필요가 있음

② 홈페이지 등의 안전한 관리를 위하여 공개용 웹서버에 방화벽 등 최소한의 접근제어 수단을 적용하고 있으나 해킹 파일 업로드 등 다양한 웹 해킹 공격시도에 대한 대응이 미흡하므로

앞으로 웹 해킹 공격시도에 대한 탐지가 가능토록 공개용 웹서버에 대해 웹 방화벽, 침입탐지시스템 등 해킹 공격에 특화된 보안장비를 도입·운영하여 다양한 홈페이지 해킹 공격에 대한 대응역량을 강화할 필요가 있음

(6) 전자금융보조업자 재무건전성 및 품질수준 평가 관리절차 개선

전자금융업자는 전자금융보조업자에 대한 재무건전성 및 서비스 품질수준을 연 1회 이상 평가하고 그 결과를 금융감독원에 보고*하여야 하나,

* 보고일 기준 계약종료가 6개월 이상 남은 계약의 경우 포함하고, 계약금액이 연간 1억 원 미만인 경우 생략 가능

전자금융보조업자에 대한 재무건전성 및 서비스 품질수준 평가 기준을 마련하지 않아 보고 대상 전자금융보조업자의 재무건전성 및 서비스 품질수준 평가결과 보고를 누락할 우려가 있으므로

앞으로 전자금융보조업자 내부 분류기준과 전자금융보조업자의 재무건전성 및 서비스 품질수준 평가절차를 내규에 반영하여 전자금융보조업자에 대한 관리·감독을 강화하고, 전자금융보조업자에 대한 평가결과의 금융감독원 보고누락 방지를 위한 관리체계를 마련·개선할 필요가 있음

(7) 전자금융사고 및 정보처리시스템 장애 보고 등 관리절차 개선

정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연되거나 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생하는 경우 지체없이 금융감독원에 보고하여야 하나,

일부 전자금융사고 및 장애에 대한 보고를 누락하였고, 장애처리 조치내역 등을 포함한 장애보고서가 별도로 작성되지 않고 있으며, 장애대응 이행현황 관리·장애조치 사후 적정성 점검 등이 미흡하므로

앞으로 전자금융사고 및 정보처리시스템 장애 보고와 관련하여 운영절차를 개선하여 보고 누락이 발생하지 않도록 하고, 장애처리 종료 후 재발방지 대책 이행 등을 정기적으로 점검하는 등 장애관리 업무를 체계적으로 관리할 필요가 있음

(8) 비상계획 및 모의훈련 운영 불합리

비상상황 시 업무지속성을 확보하기 위해 내규「OOOO OO」제OO장 및「OOOO OOOO」제OO조에 따라 재난상황에 따른 대응절차인「OOOO OO OOO」를 마련하고 연 1회 비상대응훈련을 실시하고 있으나,

OOOO년부터 OOOO년 기간 중 OOOOO OOO(OOOO), OOOO(OOOO), OO OOO(OOOO)에 대한 비상대응훈련을 실시하였으나, 일부 서비스(OO 및 OO 서비스) 대한 재해복구 훈련을 실시하지 않았고,

업무별 복구 절차에 대해「OOOO OO OOO」상 그룹웨어(OOO)에 매뉴얼을 공유토록 하고 있으나 이를 그룹웨어상 공유하지 않았고

비상연락망에 현 비상인력이 포함되지 않는 등 최신상황을 반영하여 관리하지 않아 실제 비상상황 발생 시 시스템 복구 등에 대한 상황판단이 어렵고 해당 담당자의 신속한 대응에 차질이 발생할 우려가 있으므로

비상인력을 포함한 인사이동 등에 따른 변경사항에 대해 비상연락망을 최신화하여 관리하고, 업무별 복구 절차 매뉴얼을 그룹웨어를 통해 공유하는 한편, 주요 서비스인 OO 및 OO 서비스에 대한 재해복구 훈련을 포함한 비상대응훈련을 실시하여 전자금융거래에 대한 상황별 대응능력을 높일 수 있는 훈련을 실시할 필요가 있음

(9) 정보처리시스템 성능관리 불합리

회사는 정보처리시스템에 대한 자원의 오용을 방지하고 가용성을 보장하기 위하여 내규「OOOO OO」제OO조에 따라 정보처리시스템의 성능 및 용량을 지속적으로 모니터링하고 있고

정보처리시스템의 CPU, 메모리 및 네트워크의 사용량이 임계치(OO%)를 넘거나 이상이 있는 경우 시스템 담당자에게 알려주도록 운영하여 검사대상기간(OOOO.O.O. ~ OOOO.O.O.) 중 총 OO회 이상 성능을 개선하였으나,

시스템 용량 확장 시점 예측을 위한 이용도 분석 등 시스템의 성능분석을 정기적으로 수행하지 않아 사전에 정해놓은 사용량 임계치의 적정성 및 추가 용량 확보의 필요여부를 판단하기 어렵고,

대고객·타사 제휴관련 대규모 이벤트와 신규 개발 서비스가 많은 회사의 특성을 고려할 때, 고객의 서비스 이용이 급증하는 경우 서비스 중단, 지연 등 전산 장애 사고가 발생할 우려가 있으므로

업무연속성 확보 등을 위해 정기적으로 정보처리시스템 성능과 사용량 추이, 이상 징후 발생에 대한 원인 등에 대해 종합적으로 분석하도록 관련 규정 및 업무를 개선할 필요가 있음

(10) 프로그램 및 전산원장 관리 통제 미흡

회사는 내규에 따라 프로그램 등록·변경시 개발, 테스트 및 배포 등의 절차와 전산원장의 변경 절차를 규정하고 형상관리 및 운영시스템을 이용하여 프로그램 요구사항 관리 및 변경통제 절차를 운영하고 있으며

프로그램 및 전산원장 변경을 운영시스템에 적용하기 전, 그룹웨어(OOO)를 통해 책임자가 승인을 실시하고 있으나, OOOOO, OO, OO 개발파트에서 내규상 근거 없는 권한위임을 통해 일반직원이 승인한 사례가 있으므로

앞으로 프로그램 및 전산원장 변경시 내부 책임관계를 명확하게 하기 위하여 관련 내규에 변경승인 권한위임에 대한 근거를 마련하는 등 변경승인 권한을 가진 자를 명확하게 정할 필요가 있음

(11) 제휴서비스 오인방지 등 이용자 보호대책 미흡

회사는 OOOOO 앱을 통해 전자금융업(선불, PG 등) 이외에도 보험, 투자, 교통카드 등 제휴서비스를 제공하고 있으나,

회사가 제공하는 일부 제휴서비스의 경우 서비스 주체를 명확하게 표기하지 않아 이용자가 민원 제기, 사고 신고 시 책임주체(회사)를 혼동할 우려가 있고,

회사가 대행하는 서비스 범위를 명확하게 이용자에게 고지하지 않아 관련 민원 등이 발생하고 있으므로

앞으로 제휴서비스 화면에 서비스 제공 범위 및 책임 주체를 정확히 표기하여 이용자의 오인을 방지하고, 민원·금융사고 등에 대한 책임관계를 명확히 하는 등 이용자 보호대책을 강화할 필요가 있음

(12) 가맹점 결제대금 정산관리절차 미흡

회사는 정산관리시스템을 통해 가맹점 이용자의 결제대금에서 수수료를 공제한 나머지 금액을 가맹점별 정산주기에 따라 가맹점 계좌에 지급하는 방법으로 결제대금을 정산하고 있으나,

동 시스템에는 결제대금 지급오류 발생시, 지급완료 여부를 추적·관리할 수 있는 점검절차가 마련되지 않아

OOOO.O.O. 현재 정산계좌 오류 등으로 인해 일부 결제대금(총 OO백만원)이 정산되지 않는 등 결제대금 미지급에 따른 가맹점 피해 또는 분쟁이 발생할 우려가 있으므로

앞으로 결제대금 지급오류시 지급완료 여부를 추적·관리할 수 있도록 정산관리 시스템을 개선(오류 원인 및 지급완료 여부 기록·관리 등)하고, 결제대금 미정산 가맹점을 정기적으로 점검하여 정산처리를 신속하게 완료하는 등 정산관리 절차를 개선할 필요가 있음

(13) 선불전자지급수단 운용방식 미흡

회사는 OOOOOOO과 제휴를 통해 동 OO계좌에서 선불전자지급수단(이하 'OOOOOOO')을 자동 충전하여 사용할 수 있는 신규 서비스를 출시(OOOO.O월)하였으나,

동 서비스 이용시 OOOOO 거래확인 메뉴에서 OO계좌 잔액, OO계좌 입·출금 거래기록만 조회되고 OOOOOOO의 충전·사용 등 거래기록을 조회할 수 없으며,

OOOOOOO 잔액원장과 OO계좌 잔액원장이 분리되지 않아 OOOOOOO 잔액에 OO계좌 잔액이 기록되는 문제점이 발생되고 있으므로

앞으로 OOOOOOO의 거래기록(충전, 결제, 송금 등) 및 잔액을 OO계좌 거래내용과 구분하여 조회할 수 있도록 시스템을 개선하고, 선불전자지급수단 전산원장과 OO계좌 전산원장을 분리하여 관리하는 등 관련 운용방식을 개선할 필요가 있음