공 개

의안번호	제 161 호
의 결 연 월 일	2021. 4. 28. (제 8 차)

의결사항

㈜카카오페이에 대한 부문검사 결과 조치안

금융위원회회의 안건

제 출 자	위 원 장 은 성 수
제출 연월일	2021. 4. 28.

1. 의결주문

㈜카카오페이에 대한 부문검사 결과 조치안을 <별지>와 같이 의결하며 「질서위반행위규제법」 제16조 제1항에 따라 부여된 의견제출 기한 내에 제재조치 대상자가 과태료를 납부하지 아니하고 의견제출을 하지 아니하는 경우에는 <별지>의 조치안을 그대로 확정한다.

2. 제안이유

㈜카카오페이에 대한 부문검사 결과 위법사항에 대하여 필요한 조치를 하려는 것임

3. 주요골자

‘전자금융거래 안전성 확보의무 위반’, ’전자금융거래 변경약관 게시 및 이용자 통지 위반’, ’전자금융거래 약관 보고 위반‘에 대하여 ㈜카카오페이에게 과태료를 부과하고자 함

4. 참고사항

가. 금융감독원장이 안건 상정을 요청한 사항임

나. 관계법규 : (붙임 1)

○ 「전자금융거래법」 제21조(안전성의 확보의무) 제2항
「전자금융거래법」 제24조(약관의 명시와 변경통지 등) 제3항
「전자금융거래법」 제25조(약관의 제정 및 변경) 제1항
「전자금융거래법」 제51조(과태료) 제1항제1호, 제3항제8호, 제9호

○ 「전자금융감독규정」 제7조(전자금융거래 종류별 안전성 기준)
「전자금융감독규정」 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 제1항, 제2항, 제3항, 제8항

(舊)「전자금융감독규정」 제14조의2(비중요 정보처리시스템 지정) 제1항, 제2항, 제3항

「전자금융감독규정」 제15조(해킹 등 방지대책) 제1항제3호, 제5호

「전자금융감독규정」 제17조(홈페이지 등 공개용 웹서버 관리대책) 제1항제1호, 제3호, 제4호

「전자금융감독규정」 제27조(전산원장 통제) 제1항, 제2항, 제28조(거래통제 등) 제2항, 제29조(프로그램 통제) 제7호, 제30조(일괄작업에 대한 통제) 제5호

「전자금융감독규정」 제40조(약관교부 방법 등) 제4항

「전자금융감독규정」 제41조(약관 제정 또는 변경에 따른 보고 등) 제2항

○ 「검사및제재에관한규정」 제20조(과징금 및 과태료의 부과), 별표3

○ 「질서위반행위규제법」 제16조(사전통지 및 의견제출 등) 제1항, 제17조(과태료의 부과) 제1항, 제18조(자진납부자에 대한 과태료 감경) 제1항

○ 「질서위반행위규제법 시행령」 제3조(사전통지 및 의견제출 등) 제1항 내지 제3항, 제5조(자진납부자에 대한 과태료 감경)

다. 제재내용 공개안 (붙임 2)

라. 관계부서 협의

○ 제13차 제재심의위원회(2021.4.1.) 심의필

<별지>

㈜카카오페이에 대하여 다음과 같이 조치한다.

- 다 음 -

1. 조치내용

□ 기관에 대한 조치

○ 과태료 6,960만원 부과*

* 과태료 부과 사전통지 후 의견제출 기한내 자진납부시 「질서위반행위규제법」 제18조에 따라 부과금액의 20%를 감경

- 조치사유 : 전자금융거래 안전성 확보의무 위반, 전자금융거래 변경약관 게시 및 이용자 통지 위반, 전자금융거래 약관 보고 위반

- 법적근거 : 「전자금융거래법」 제21조제2항, 제24조제3항, 제25조제1항, 제51조 제1항제1호, 제3항제8호, 제9호
「전자금융감독규정」 제7조, 제14조의2제1항, 제2항, 제3항, 제8항, 제15조제1항제3호, 제5호, 제17조제1항제1호, 제3호, 제4호, 제27조제1항, 제2항, 제28조제2항, 제29조제7호, 제30조제5호, 제40조제4항, 제41조제2항
(舊)「전자금융감독규정」 제14조의2제1항, 제2항, 제3항

2. 조치사유

가. 전자금융거래 안전성 확보의무 위반

(1) 클라우드컴퓨팅서비스 이용절차 등 수행 위반

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조 및 제14조의2 제1항부터 제3항, (舊)「전자금융감독규정」 제14조의2제1항부터 제3항에 의하면 전자금융업자는 비중요 정보처리시스템 지정 또는 클라우드컴퓨팅서비스(이하 '클라우드')를 이용하고자 하는 경우에 <비중요 정보처리시스템 지정절차> 또는 <클라우드 이용절차>를 수행하여야 하는데도,

< 비중요 정보처리시스템 지정절차 >

① 자체적으로 수립한 정보자산 중요도 평가기준에 따른 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은 정보처리시스템을 비중요 정보처리시스템으로 지정(단, 고유식별정보 또는 개인신용정보를 처리하는 경우 지정 불가)
② 비중요 정보처리시스템 지정시 정보보호위원회 심의·의결
③ 비중요 정보처리시스템을 지정한 날로부터 7일 이내에 금융감독원 보고

< 클라우드컴퓨팅서비스 이용절차 >

① 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가
② 「전자금융감독규정」<별표 2의2>의 항목을 포함한 클라우드컴퓨팅서비스제공자의 건전성 및 안전성 등 평가
③ 「전자금융감독규정」<별표 2의3>에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수
④ ①부터 ③까지의 평가결과 및 자체 업무 위수탁 운영기준에 대하여 정보보호위원회의 심의·의결
⑤ '고유식별정보 또는 개인신용정보를 처리하는 경우' 또는 '전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 경우'에 해당한다고 평가하는 경우에는 실제로 이용하는 날의 7영업일 이전에 금융감독원장에게 보고

○ ○○○○○는 OOOO.O.O. ~ OOOO.O.O. 기간 중 OOOO 시스템을 OOOOOO 클라우드 환경에서 사용하고 있었음에도 <비중요 정보처리시스템 지정절차> 또는 <클라우드 이용절차>를 수행하지 않은 사실이 있음

(2) 내부 업무용시스템, 정보처리시스템 등의 망분리 이행 위반

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조 및 제15조제1항제3호에 의하면 전자금융업자는 내부통신망과 연결된 내부 업무시스템을 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속을 금지하여야 하고,

「전자금융감독규정」 제15조제1항제5호에 의하면 회사의 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 하며,

클라우드 제공자의 전산실 내에 위치한 정보처리시스템에 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서도 인터넷 등 외부통신망으로부터 물리적으로 분리*하여야 하는데도,

* 「전자금융감독규정」 제14조의2제8항은 클라우드컴퓨팅 서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서만 망분리 예외를 둔다는 조항으로, 클라우드컴퓨팅서비스 제공자의 정보처리시스템에 직접 접속하는 회사 전산실의 단말기는 「전자금융감독규정」 제15조제1항제5호에 따라 망분리 적용대상임

○ 회사는 OOOO.O.O. ~ OOOO.O.O. 기간 중 내부통신망에 연결된 본사 임직원의 업무단말기와 내부 업무용시스템에 대해 망분리* 이행을 완료하지 않고 인터넷 등 외부통신망과 연결하여 운영하는 등 외부통신망과 분리·차단 및 접속을 금지하지 않고 운영**하고 있으며

* 망분리 도입 현황(도입일) : 임직원 업무단말기 및 내부 업무용시스템(ㅇㅇㅇㅇ.ㅇ.ㅇ.), 정보처리시스템과 직접 접속 단말기(ㅇㅇㅇㅇ.ㅇ.ㅇㅇ.)

** ① 모든 임직원이 인터넷 접속이 허용(음란·도박 등 차단)된 업무단말기(내부통신망에 연결)에서 내부통신망에 연결된 내부 업무용시스템 ㅇ개(ㅇㅇㅇ ㅇㅇㅇㅇ, ㅇㅇ·ㅇㅇ ㅇㅇㅇ)를 사용하고 있음(다만, 임직원이 전자금융업무시스템 ㅇㅇ개 등 총 ㅇㅇ개 내부 업무시스템 접속 시에는 가상화PC를 통해 접속)

② 가상화PC에서 접속하는 내부 업무용시스템 ○○개(○○, ○○ ○○○ 등 전자금융업무 ○○개, 배송, 배너 어드민 등 기타 업무 ○○개)는 ○○ 이미지 ○○○(콘텐츠 전송 네트워크, Content Delivery Network) 홈페이지를 연결(프록시 경유)하여 운영

○ 회사 전산실 내에 위치한 일부 정보처리시스템(OO·OO·OO 등의 업무처리 및 OO OOOOO OO 서버)에 대해서 인터넷(OO, OO, OOO, OOO 등의 이미지CDN, OO·OO OOOOO 등 홈페이지) 등 외부통신망과 물리적으로 분리하지 않고 연결하여 운영*하는 한편,

* 주전산·DR전산센터의 페이·머니·결제·정산·청구·인증 등 업무처리 서버 ○○대, 개발·운영 라이브러리 배포 서버 ○○대 등 정보처리시스템 ○○대에 대해서 ○○, ○○, ○○○, ○○○○○ 및 ○○○ 등의 이미지 ○○○, 개발·운영 관련 오픈소스·라이브러리 등 홈페이지 ○○개와 물리적으로 분리하지 않고 연결

○ 회사 전산실의 정보처리시스템(OOOOOOOO)에 개발 목적으로 직접 접속하는 단말기에 대해서 인터넷 등 외부통신망과 물리적으로 분리하지 않고 연결하여 운영*하고 있으며,

* 인터넷 접속이 허용(음란·도박 등 차단)된 전산직원의 업무용 단말기 ○○○대에서 주전산센터의 ○○○시스템 ○대에 소스코드형상관리기능(○○○클라이언트)이 내장된 개발도구(○○○○)로 직접 연결

- 클라우드 제공자(OOO)의 정보처리시스템(OO, OO·OO·OO 설정관리콘솔)에 운영, 개발, 보안 목적으로 직접 접속하는 회사의 단말기에 대해서도 인터넷 등 외부통신망으로부터 물리적으로 분리하지 않고 연결하여 운영한 사실이 있음*

* 인터넷 접속이 허용(음란·도박 등 차단)된 전산직원의 업무용 단말기 ○대에서 ○○○클라우드서비스의 프로모션 ○대·법무○대·인증키관리(KMS) ○대·블록체인(○○○○) ○대 등 서버(○○○ ○○○) ○○대, 서버·통신·보안설정을 위한 ○○○ 관리콘솔 ○개 등 정보처리시스템 ○○대에 대해 ○○○, ○○○○○○○, ○○○○, ○○○○○○워크벤치로 직접 연결

(3) 홈페이지 등 공개용 웹서버 관리 대책 이행 위반

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조 및 제17조제1항제1호, 제3호, 제4호에 의하면 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간")에 설치하고 네트워크 및 웹 접근제어 수단으로 보호하여야 하고,

공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한하여야 하며, DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니하여야 하는데도 (다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 함)

○ OOOO.O.O. ~ OOOO.O.O. 기간 중, OOO 클라우드의 공개용 웹서버(프로모션 이벤트 홈페이지)를 내부통신망과 분리하여 내부통신망과 외부통신망 사이의 독립된 통신망(DMZ구간)에 설치하지 아니하고 내부통신망에 설치하면서 웹 접근제어 수단(침입탐지시스템의 웹접근제어 규칙 등)으로 보호하지 않고 운영*하고

* ○○○○.○.○○.부터 아마존클라우드의 프로모션 홈페이지 공개용 웹서버 ○대(각 ○○○ 인스턴스에 웹서버SW와 웹어플리케이션서버 SW를 같이 설치)를 DB서버(MySQL RDS DB인스턴스)가 위치한 내부통신망(Private Subnet)에 설치하여 운영하면서 네트워크 접근제어 수단(○○○의 NACL, Security Group)으로만 접근제어 실시

○ 회사 전산실 및 클라우드의 공개용 웹서버(OO, OOOO, OOOO 홈페이지 공개용 웹서버 등)에서 시험·개발도구(gcc, g++, make 등)의 사용을 제한하지 않고 운영*하고 있으며

* 공개용 웹서버 ○○○대(회사 전산실의 머니 홈페이지 등 ○○○대, ○○○ 클라

우드의 프로모션 홈페이지 ○대)에 설치한 시험·개발도구 ○○개(gcc, g++, make, libssl-dev, lipcre3- dev, libc-dev, libc6-dev 등)의 사용을 ○○○○.○.○.부터 제한하지 않음(제공하는 홈페이지 서비스를 제외한 다른 서비스는 없음)

○ DMZ구간 내의 공개용 웹서버(OO·OOOO 홈페이지)의 거래로그에 이용자 OOOO 및 OOOOOO를 저장하여 관리하면서 암호화하지 않은 사실이 있음*

* ① 머니 공개용 웹서버 ○대(○○○○-○○○○.com 서비스)의 거래로그(application_18 080.log, pay-moneny-apigw_access_json.log)에 계좌송금시 이용자로부터 입력받는 계좌번호를 ○○○○.○.○○.~○○.○.까지 평문으로 저장·관리

② 페이카드 공개용 웹서버 ○대(○○○○○○○○.com 서비스)의 거래로그(○○○○○○○-more_access.log, ○○○○○-more_access_json.log)에 이용자로부터 본인인증을 위해 입력받는 휴대전화번호를 ○○○○.○.○○.~○○.○○.까지 평문으로 저장·관리

③ 각 공개용 웹서버의 거래로그에 이용자의 계좌번호와 휴대전화번호가 수개월간 저장·관리되었으나 2019년 하반기 홈페이지 취약점 분석·평가 과정에서 발견되어 해당서버와 백업장치 등에 저장된 모든 계좌번호 및 휴대전화번호를 삭제하고 웹서버 프로그램을 수정하여 해당 정보가 남지 않도록 조치

(4) 프로그램 및 전산원장 관리통제 위반

□ 「전자금융거래법」 제21조 제2항 및 「전자금융감독규정」 제7조, 제27조 제1항, 제2항, 제28조 제2항, 제29조 제7호, 제30조 제5호에 의하면 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 변경내용의 정당여부에 대해 제3자 확인 등을 포함한 별도의 변경절차를 수립·운용하여야 하고 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 하여야 하며,

일괄작업(batch)의 수행을 위하여 책임자가 일괄작업 수행자의 주요업무 관련 행위를 모니터링하여야 하고 프로그램 반출, 실행 프로그램의 생성 및 운영시스템 등록을 전산자료 관리자 등 해당 프로그램 담당자 이외의 자가 수행하여야 하는데도

○ OOOO.O.O. ~ OOOO.O.O. 기간 중 전산원장 변경내용의 정당 여부에 대해 내부감사 등 제3자의 승인없이 책임자의 승인만을 통해 변경을 실시*하였고, 전산원장의 중요작업에 대한 책임자의 이중확인 및 일괄작업 수행자의 주요업무 관련 행위에 대한 책임자의 모니터링을 수행하지 않았으며,

* ○○○○○.○월 ○○○건의 전산원장 변경 수행

○ OOOO.O.O. ~ OOOO.O.O. 기간 중 프로그램 반출 및 운영시스템 등록을 해당 프로그램 담당 개발자가 직접 배포*한 사실이 있음

* ○○○○○.○월 ○○○건의 프로그램 등록·변경 중 ○○○건

나. 전자금융거래 변경약관 게시 및 이용자 통지 위반

□ 「전자금융거래법」 제24조 제3항 및 「전자금융감독규정」 제40조 제4항에 의하면 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 그 시행일 1월전에 변경되는 약관을 해당 전자금융거래를 수행하는 전자적 장치에 게시하고 이용자에게 통지하여야 하는데도,

○ 회사는 OOOO.O.O. ‘OOOOO 이용약관’(이하 ‘약관’)을 제정한 이후 현재까지 총 O차례* 약관을 변경하면서

* 약관개정시행일 : ①****.*.**., ②****.*.**., ③****.*.**., ④****.**.**., ⑤****.*.**., ⑥****.*.*., ⑦****.*.*., ⑧****.*.*., ⑨****.**.*.

변경된 약관을 전자적 장치에 지연 게시(○회)하거나, 통지기한

내에 이용자에게 통지하지 아니한(ㅇ회) 사실이 있음*

* 전자적 장치 지연 게시 ㅇ건은 모두 이용자 통지 미실시

※ ‘ㅇㅇㅇㅇㅇ 이용약관’의 전자적 장치 게시 및 이용자 통지 위반 내역

구분	개정 차수	약 관 시행일	전자적장치 게시일 (게시지연일)	이용자 통지일 (통지지연일)	위반 사항
(1)	①	****.**.**.	****.**.**. (24일)	×	약관 지연게시(24일 지연) 및 이용자 미통지
(2)	②	****.**.**.	****.**.**. (24일)	×	약관 지연게시(24일 지연) 및 이용자 미통지
(3)	③	****.**.**.	****.**.**.	×	이용자 미통지
(4)	④	****.**.**.	****.**.**. (23일)	×	약관 지연게시(23일 지연) 및 이용자 미통지
(5)	⑤	****.**.**.	****.**.**. (22일)	×	약관 지연게시(22일 지연) 및 이용자 미통지
(6)	⑥	****.**.**.	****.**.**.	2019.08.02. (1일)	이용자 지연통지(1일 지연) 및 일부 이용자 미통지[1]

1) 2019.8.1. 기준 전체 이용자(27,918,853명, 휴면계정 이용자 제외)가 아닌 ㅇㅇㅇㅇㅇㅇㅇㅇㅇ(‘ㅇㅇㅇㅇㅇ’)를 등록한 이용자(ㅇㅇㅇㅇㅇㅇㅇㅇ명)에게만 통지하여 ㅇㅇㅇㅇㅇㅇㅇㅇ명에게 약관변경 사실이 통지되지 않음

다. 전자금융거래 약관 보고 위반

□ 「전자금융거래법」 제25조제1항 및 「전자금융감독규정」 제41조제2항에 의하면 금융회사 또는 전자금융업자가 전자금융거래에 관한 약관을 제정하거나 변경하고자 하는 경우에는 미리 금융위원회에 보고* 하여야 하는데도,

* 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융위원회가 정하는 경우에는 약관의 제정 또는 변경 후 10일 이내에 금융위원회에 보고 가능

○ 회사는 OOOO.O.O. ‘OOOOO 이용약관’(이하 ‘약관’)을 제정한 이후 현재까지 총 O차례 약관을 변경하면서

* 약관개정시행일 : ①****.*.**., ②****.*.**., ③****.*.**., ④****.*.**., ⑤****.*.**., ⑥****.*.**., ⑦****.*.**., ⑧****.*.**., ⑨****.*.**.

제정 약관은 시행일(OOOO.O.O.)로부터 O일 후에 금융위원회에 지연하여 보고(OOOO.O.O.)하였고, 약관개정시행일이 OOOO.O.O. 등 약관(O건)은 금융위원회에 보고하지 않은 사실이 있음

※ ‘ㅇㅇㅇㅇㅇ 이용약관’의 약관 보고 위반 내역

구분	개정 차수	약관시행일	약관보고일	약관 변경 내용	보고 기한	위반 사항
(1)	제정	****.**.**.	****.**.**.	-	시행일 45일 전	지연 보고
(2)	①	****.**.**.	×	서비스 이용연령 확대(15세→14세)	시행일로부터 10일 이내	미보고
(3)	③	****.**.**.	×	휴대폰 간편결제 서비스 제외	시행일 45일 전	미보고
(4)	④	****.**.**.	×	ㅇㅇㅇㅇㅇ → ㅇㅇㅇㅇㅇ머니 (단순 명칭 변경)	시행일로부터 10일 이내	미보고
(5)	⑤	****.**.**.	×	ㅇㅇㅇㅇㅇ 서비스 이용절차(제7조), ㅇㅇㅇㅇㅇ (제10조) 등 조항 수정	시행일 45일 전	미보고

(붙임 1)

관계 법규

【전자금융거래법】

제21조(안전성의 확보의무) ① (생략)

② 금융회사등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및 「전자서명법」에 의한 인증서의 사용 등 인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.

③~④ (생략)

제24조(약관의 명시와 변경통지 등) ①~②(생략)

③ 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 변경되는 약관의 시행일 1월 전에 금융위원회가 정하는 방법에 따라 이를 게시하고 이용자에게 알려야 한다. 다만, 법령의 개정으로 인하여 긴급하게 약관을 변경하는 때에는 금융위원회가 정하는 방법에 따라 이를 즉시 게시하고 이용자에게 알려야 한다.

④ (생략)

제25조(약관의 제정 및 변경) ① 금융회사 또는 전자금융업자가 전자금융거래에 관한 약관을 제정하거나 변경하고자 하는 경우에는 미리 금융위원회에 보고하여야 한다. 다만, 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융위원회가 정하는 경우에는 약관의 제정 또는 변경 후 10일 이내에 금융위원회에 보고할 수 있다.

②~④ (생략)

제39조(감독 및 검사) ① 금융감독원은 금융위원회의 지시를 받아 금융회사 및 전자금융업자에 대하여 이 법 또는 이 법에 의한 명령의 준수여부를 감독한다.

②~⑤ (생략)

⑥ 금융위원회는 금융회사 또는 전자금융업자가 이 법 또는 이 법에 따른 명령을 위반하여 금융회사 또는 전자금융업자의 건전한 운영을 해할 우려가 있다고 인정하는 때에는 금융감독원장의 건의에 따라 다음 각 호의 어느 하나에 해당하는 조치를 하거나 금융감독원장으로 하여금 제1호 내지 제3호에 해당하는 조치를 하게 할 수 있다.

1. 위반행위에 대한 시정명령
2. 금융회사 또는 전자금융업자에 대한 주의 또는 경고

3. 임원과 직원에 대한 주의, 경고 또는 문책의 요구
4. 임원의 해임권고 또는 직무정지의 요구

제51조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

1. 제21조 제1항 또는 제2항을 위반하여 선량한 관리자로서의 주의를 다하지 아니하거나 금융위원회가 정하는 기준을 준수하지 아니한 자

2.~4. (생략)

② (생략)

③ 다음 각호의 어느 하나에 해당하는 자(제1호, 제6호부터 제8호까지 및 제10호의 경우에는 제28조제4항에 따라 해당 규정을 준용하는 선불전자지급수단을 발행하는 자를 포함한다)에게는 1천만원 이하의 과태료를 부과한다.

1.~7. (생략)

8. 제24조제1항 또는 제3항을 위반하여 약관의 명시, 설명, 교부를 하지 아니하거나 게시 또는 통지하지 아니한 자
9. 제25조제1항을 위반하여 금융위원회에 보고하지 아니한 자

10.~12. (생략)

④ (생략)

【전자금융거래법시행령】

제33조(과태료의 부과기준) 법 제51조제1항부터 제3항까지의 규정에 따른 과태료의 부과기준은 별표 3과 같다.

[별표 3]

과태료의 부과기준(제33조 관련)

1. 일반기준

금융위원회는 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 제2호에 따른 과태료 금액을 감경 또는 면제하거나 2분의 1의 범위에서 가중할 수 있다. 다만, 가중하는 경우에도 법 제51조제1항부터 제3항까지의 규정에 따른 과태료 금액의 상한을 초과할 수 없다.

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	금액
가. ~ 마. (생략)		

바. 법 제21조제2항을 위반하여 금융위원회가 정하는 기준을 준수하지 않은 경우	법 제51조 제1항제1호	5,000
사. ~ 너. (생략)		
더. 법 제24조제1항 또는 제3항을 위반하여 약관의 명시, 설명, 교부를 하지 않거나 게시 또는 통지하지 않은 경우	법 제51조 제3항제8호	600
러. 법 제25조제1항을 위반하여 금융위원회에 보고하지 않은 경우	법 제51조 제3항제9호	600
머. ~ 터. (생략)		

【전자금융감독규정】

제7조(전자금융거래 종류별 안전성 기준) 법 제21조 제2항의 "금융위원회가 정하는 기준"이라 함은 다음 각 호의 내용에 관하여 제8조 부터 제37조에서 정하는 기준을 말한다

1. 인력, 조직 및 예산 부문
2. 건물, 설비, 전산실 등 시설 부문
3. 단말기, 전산자료, 정보처리시스템 및 정보통신망 등 정보기술부문
4. 그 밖에 전자금융업무의 안전성 확보를 위하여 필요한 사항

(舊)**제14조의2(비중요 정보처리시스템 지정)** ① 금융회사 또는 전자금융업자는 자체적으로 수립한 정보자산 중요도 평가기준에 따라 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은 정보처리시스템을 비중요 정보처리시스템으로 지정할 수 있다. 다만, 개인의 고유식별정보 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없다. <신설 2016.10.5., 2016.10.5. 시행>

② 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템 지정시 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.<신설 2016.10.5., 2016.10.5. 시행>

③ 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템을 지정한 날로부터 7일 이내에 금융감독원장이 정하는 양식에 따라 정보자산 중요도 평가기준, 지정 결과, 관리 방안 등을 포함한 보고서를 금융감독원에 제출하여야 한다.<신설 2016.10.5., 2016.10.5. 시행>

④ (생략)

⑤ 제1항의 비중요 정보처리시스템만 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다.<신설 2016.10.5., 2016.10.5. 시행>

제14조의2(클라우드컴퓨팅서비스 이용절차 등) ① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 함<개정 2018.12.21., 2019.1.1. 시행>

1. 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가
2. <별표 2의2>의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등의 평가
3. <별표 2의3>에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

② 금융회사 또는 전자금융업자는 제1항의 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

③ 금융회사 또는 전자금융업자는 제1항 제1호에 따라 다음 각 호의 어느 하나에 해당한다고 평가하는 경우에는 클라우드컴퓨팅서비스를 실제로 이용하려는 날의 7영업일 이전에 금융감독원장이 정하는 양식에 따라 제4항 각호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다. 이 경우 「금융회사의 정보처리 업무 위탁에 관한 규정」제7조 제1항부터 제3항까지의 규정에 따라 보고한 것으로 본다.

1. 고유식별정보 또는 개인신용정보를 처리하는 경우
2. 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 경우

④~⑦ (생략)

⑧ 제2항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자는 제외한다)가 제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.

⑨ 그 밖에 금융회사 또는 전자금융업자의 클라우드컴퓨팅서비스 이용에 대해서는 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따른다.

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1.~2. (생략)

3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다) <개정 2013.12.3>
4. (생략)

5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)

②~⑥ (생략)

제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.<개정 2013.12.3>

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것
2. (생략)
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

제27조(전산원장 통제) ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용하여야 한다.

② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.

③~⑤ (생략)

제28조(거래통제 등) ① (생략)

② 금융회사 또는 전자금융업자는 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 해야 한다.<개정 2013.12.3.>

제29조(프로그램 통제) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다.<개정 2013.12.3>

1. ~ 6. (생략)
7. 프로그램 반출, 실행프로그램의 생성 및 운영시스템 등록은 전산자료 관리자 등 해당 프로그램 담당자 이외의 자가 수행할 것
8. ~ 10. (생략)

제30조(일괄작업에 대한 통제) 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다.<개정 2013.12.3>

1. ~ 4. (생략)

5. 책임자는 일괄작업 수행자의 주요업무 관련 행위를 모니터링할 것

제40조(약관교부 방법 등) ①~③ (생략)

④ 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 그 시행일 1월 전에 변경되는 약관을 해당 전자금융거래를 수행하는 전자적 장치(해당 전자적 장치에 게시하기 어려울 경우에는 이용자가 접근하기 용이한 전자적 장치로서 당해 금융회사 등이 지정하는 대체장치를 포함한다. 이하 이 조에서 같다)에 게시하고 이용자에게 통지하여야 한다. 다만, 이용자가 이의를 제기할 경우 금융회사 또는 전자금융업자는 이용자에게 적절한 방법으로 약관 변경내용을 통지하였음을 확인해 주어야 한다.

⑤ (생략)

제41조(약관 제정 또는 변경에 따른 보고 등) ① 법25조제1항 단서에서 "금융위원회가 정하는 경우란" 다음 각호와 같다.

1. 이용자의 권익을 확대하거나 의무를 축소하기 위한 약관의 변경
2. 금융감독원장에게 보고된 약관의 내용과 동일하거나 유사한 약관의 제정 또는 변경
3. 그 밖에 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융감독원장이 정하는 약관의 제정 또는 변경

② 금융회사 또는 전자금융업자가 전자금융거래 약관을 제정 또는 변경하고자 하는 경우에는 해당 약관 및 약관내용을 이해하는데 필요한 관련서류를 시행예정일 45일 전까지 금융감독원장에게 제출하여야 한다. 이 경우 약관 및 관련서류는 전자문서로 제출할 수 있다.

③ 금융감독원장은 제2항의 규정에 따라 제출받은 약관을 심사하고 건전한 금융거래 질서의 유지를 위하여 약관내용의 변경이 필요하다고 인정하는 경우 해당 금융회사 또는 전자금융업자에 대하여 약관의 변경을 권고할 수 있음

④ (생략)

부 칙<2013.12.3>

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제15조제1항제3호의 규정은 「은행법」에 따라 인가를 받아 설립된 은행은 2016년 1월 1일부터, 그 외의 자는 2017년 1월 1일부터 시행하고, 같은 항 제5호의 규정은 2015년 1월 1일부터 시행한다.

부 칙<제2018-36호, 2018.12.21>

제1조(시행일) 이 규정은 2019년 1월 1일부터 시행한다.

제2조(클라우드컴퓨팅서비스 이용절차 등에 관한 적용례) 제14조의2의 개정규정은 이 규정 시행 이후 클라우드컴퓨팅서비스를 이용하고자 하는 금융회사 또는 전자금융업자부터 적용한다.

【금융기관검사및제재에관한규정】

제14조 (검사결과의 통보 및 조치) ① 감독원장은 금융기관에 대한 검사결과를 검사서에 의해 당해 금융기관에 통보하고 필요한 조치를 취하거나 당해 금융기관의 장에게 이를 요구할 수 있다.

② 제1항의 규정에 의한 검사서 작성 및 검사결과 조치요구사항은 다음 각 호와 같이 구분한다.

1. (생략)
2. 지적사항

가. 문책사항

금융기관 또는 금융기관의 임직원이 금융관련 법규를 위반하거나 금융기관의 건전한 영업 또는 업무를 저해하는 행위를 함으로써 신용질서를 문란하게 하거나 당해기관의 경영을 위태롭게 하는 행위로서 과태료· 과징금 부과, 기관 및 임원에 대한 주의적 경고 이상의 제재, 직원에 대한 면직·업무의 전부 또는 일부에 대한 정직·감봉·견책에 해당하는 제재의 경우

나. ~ 마. (생략)

3. (생략)

③~④ (생략)

제18조(임원에 대한 제재) ① 금융위설치법, 금융산업구조개선법 및 금융업관련법의 규정 등에 의거 금융기관의 임원에 대하여 취할 수 있는 제재의 종류 및 사유는 다음 각호와 같다.

1.~4. (생략)

5. 주의

제4호에 해당되나 위법·부당행위의 동기, 목적, 방법, 수단, 사후수습 노력 등을 고려할 때 정상참작의 사유가 크거나 위법·부당행위의 정도가 제4호의 제재에 해당되는 경우보다 경미한 경우

② 감독원장은 금융기관의 임원이 제1항 각호에 해당하는 사유가 있는 경우에는 당해 임원에 대하여 제1항제1호 및 제2호에 해당하는 조치를 취할 것을 금융위에 건의하여야 하며, 제1항제3호 내지 제5호에 해당하는 조치를 취할 수 있다.

③~⑥ (생략)

제19조(직원에 대한 제재) ① 감독원장은 금융관련법규에 따라 다음 각호의 어느 하나에 해당하는 경우 금융위에 금융기관의 직원에 대한 면직요구 등을 건의하거나 당해 금융기관의 장에게 소속 직원에 대한 면직, 정직, 감봉, 견책 또는 주의 등의 제재조치를 취할 것을 요구할 수 있다.

1. 금융기관의 건전성 또는 금융소비자 권익을 크게 훼손하거나 금융질서를 문란하게 한 경우
2. 당해 금융기관의 내부통제체제가 취약하거나 제2항에 의한 자율처리필요사항이 과거에 부적정하게 처리되는 등 자율처리필요사항을 통보하기에 적합하지 않다고 판단되는 경우

②~③ (생략)

제20조(과징금 및 과태료의 부과) ① 감독원장은 금융기관 또는 그 임직원이 금융업 관련법에 정한 과징금 또는 과태료의 부과대상이 되는 위법행위를 한 때에는 금융위에 과징금 등의 부과를 건의하여야 한다. 당해 위법행위가 법령 등에 따라 부과면제 사유에 해당한다고 판단하는 경우에는 부과 면제를 건의하여야 한다.

② (생략)

③ 제1항에 의하여 과징금 또는 과태료의 부과를 금융위에 건의하는 경우에는 <별표2> 과징금 부과기준, <별표3>과태료 부과기준 및 <별표6>업권별 과태료 부과기준에 의한다.

<별표 3> 舊 과태료 부과기준(2017.10.19. 개정 전)

3. 예정금액의 산정

과태료 부과대상자에 대하여 위반행위의 동기 및 결과를 고려하여 예정금액을 다음 표와 같이 산정한다.

동기 / 위반결과	고의	과실
중대	법정최고금액의 100%	법정최고금액의 75%
보통	법정최고금액의 75%	법정최고금액의 50%
경미	법정최고금액의 50%	법정최고금액의 25%

※ 위반결과를 고려함에 있어 그 구분기준의 내용은 다음과 같다.

(1) 중 대 : 사회·경제적 물의를 야기하거나 금융기관 또는 금융소비자에 손실을 초래한 경우 및 금융기관의 건전한 운영을 위한 기본적 의무 위반 등으로 금융질서를 저해하는 경우 등을 의미
(2) 보 통 : '중대', '경미'에 해당하지 않는 경우를 의미
(3) 경 미 : 단순법규 위반 등을 의미

<별표 3> 과태료 부과기준(2017.10.19. 개정)

1. 목 적

이 기준은「은행법」등 금융업관련법령에서 정한 과태료를 부과함에 있어 필요한 사항을 정함에 그 목적이 있다.

2. 과태료 산정방식

가. 금융업관련법상 정해진 과태료부과 대상자별 법정최고금액(금융업관련법령 등에서 위반행위의 종류별로 부과금액을 정하고 있는 경우 그 규정된 해당금액을 말한다. 이하 같다.)을 과태료부과 기준금액으로 한다.

나. (생략)

다. 위반행위의 동기 및 결과를 고려하여 법정최고금액의 일정비율로 예정금액(동일인의 2개 이상의 위반행위가 경합하여 과태료를 각각 부과하는 경우 각 위반행위별 예정금액을 말한다. 이하 같다)을 산정한다.

라.~바. (생략)

3. 예정금액의 산정

가. 과태료 부과대상자에 대하여 위반행위의 동기 및 결과를 고려하여 예정금액을 다음 표와 같이 산정한다.

동기 / 위반결과	상	중	하
중대	법정최고금액의 100%	법정최고금액의 80%	법정최고금액의 60%
보통	법정최고금액의 80%	법정최고금액의 60%	법정최고금액의 40%
경미	법정최고금액의 60%	법정최고금액의 40%	법정최고금액의 20%

※ 위반결과를 고려함에 있어 그 구분기준의 내용은 다음과 같다.

(1) 중 대 : 당해 또는 유사 위반행위가 언론에 공표되어 당해 금융기관은 물론 금융업계의 공신력을 실추시킨 경우 등 사회·경제적 물의를 야기한 경우 또는 금융기관·금융거래자에 손실을 초래한 경우 또는 금융기관의 건전한 운영을 위한 기본적 의무 위반 등으로 금융질서를 저해하는 경우 등을 의미

(2) 보 통 : '중대', '경미'에 해당하지 않는 경우를 의미

(3) 경 미 : 당해 또는 유사 위반행위가 언론에 공표되어 당해 금융기관의 공신력을 실추시킨 정도의 사회·경제적 파급효과가 없고 금융거래자에 피해가 없는 경우 등을 의미

※ 구분기준 중 위반동기의 내용은 다음과 같다.

(1) 상 : 위반행위가 위반자의 고의에 의한 경우로서 위반행위의 목적, 동기, 당해 행위에 이른 경위 등에 특히 참작할 사유가 없는 경우

(2) 중 : 위반행위가 위반자의 고의에 의한 경우로서 위반행위의 목적, 동기, 당해 행위에 이른 경위 등에 특히 참작할 사유가 있는 경우 또는 위반행위가 위반자의 중과실에 의한 경우

(3) 하 : 상 또는 중에 해당하지 않는 경우

【금융기관검사및제재에관한규정시행세칙】

제45조(직원에 대한 제재) ① 규정 제5조 및 제19조에 의한 금융기관 직원에 대한 제재의 종류 및 사유는 다음과 같다.

1.~3. (생략)

4. 견책

제3호 각목의 1에 해당되나 정상참작의 사유가 있거나 위법.부당행위의 정도가 비교적 가벼운 경우

5. 주의

정상참작의 사유가 크거나 위법.부당행위의 정도가 상당히 경미한 경우

②~③ (생략)

제46조(임직원 등에 대한 제재기준) ① 위법·부당행위 관련 임직원 등을 제재함에 있어서는 별표 2의 제재양정기준과 다음 각 호의 사유를 참작한다.

1. 제재대상자의 평소의 근무태도, 근무성적, 개전의 정 및 동일·유사한 위반행위에 대한 제재 등 과거 제재사실의 유무
2. 위법·부당행위의 동기, 정도, 손실액규모 및 금융질서 문란·사회적 물의야기 등 주위에 미친 영향
3. 제재대상자의 고의, 중과실, 경과실 여부
4. 사고금액의 규모 및 손실에 대한 시정·변상 여부
5. 자진신고, 검사업무에의 협조정도 등 사후수습 및 손실경감을 위한 노력 여부
6. 경영방침, 경영시스템의 오류, 금융·경제여건 등 내·외적 요인과 귀책판정과의 관계

② 금융실명법을 위반한 행위 등 특정 위법·부당행위에 대한 제재는 별표 3의 금융업종별·위반유형별 제재양정기준에 의한다. 다만, 제1항 등 여타 제재기준을 참작하여 제재를 가중하거나 감경하는 등 제재수준을 정할 수 있다.

제46조의3(미등기 임원에 대한 제재) 이사.감사와 사실상 동등한 지위에 있는 미등기 임원에 대하여는 임원에 대한 제재기준을 준용하여 제재양정을 결정하며, 직원에 대한 제재조치를 부과한다.

제52조(관련자의 구분) ① 위법.부당행위를 행한 임직원에 대하여 신분상의 조치를 함에 있어서는 책임의 성질.정도 등에 따라 관련자를 다음 각호와 같이 구분한다.

1. 행위자 : 위법.부당한 업무처리를 실질적으로 주도한 자
2. 보조자 : 행위자의 의사결정을 보조하거나 지시에 따른 자
3. 지시자 : 위법.부당행위를 지시 또는 종용한 자(사실상의 영향력을 행사하는 상위직급자를 포함한다)
4. 감독자 : 위법.부당행위가 발생한 업무를 지도.감독할 지위에 있는 자

② 제1항에서 정한 행위자와 감독자를 판단할 수 있는 세부기준은 다음 각 호와 같다.

1. 행위자 : 업무의 성질과 의사결정의 관여정도를 고려하여 실질적인 최종 의사결정권을 가지는 자
2. 감독자 : 당해 금융기관 직제를 기준으로 행위자에 대해 관리·감독할 지위에 있는 자. 직제상 감독자가 아닌 경우라 하더라도 실질적으로 행위자에게 영향력을 미치는 때에도 또한 같다.

③ 제1항에 정한 보조자 및 감독자에 대하여는 다음 각호의 사항을 감안하여 행위자에 대한 제재보다 1단계 내지 3단계 감경할 수 있다.

1. 위법·부당행위의 성격과 규모
2. 감독자의 직무와 감독대상 직무와의 관련성 및 관여정도
3. 보조자의 위법·부당행위에의 관여 정도

【질서위반행위규제법】

제16조(사전통지 및 의견 제출 등) ① 행정청이 질서위반행위에 대하여 과태료를 부과하고자 하는 때에는 미리 당사자에게 대통령령으로 정하는 사항을 통지하고, 10일 이상의 기간을 정하여 의견을 제출할 기회를 주어야 한다. 이 경우 지정된 기일까지 의견제출이 없는 경우에는 의견이 없는 것으로 본다.

제17조(과태료의 부과) ① 행정청은 제16조의 의견 제출 절차를 마친 후에 서면(당사자가 동의하는 경우에는 전자문서를 포함한다. 이하 이 조에서 같다)으로 과태료를 부과하여야 한다.

제18조(자진납부자에 대한 과태료 감경) ① 행정청은 당사자가 제16조에 따른 의견 제출 기한 이내에 과태료를 자진하여 납부하고자 하는 경우에는 대통령령으로 정하는 바에 따라 과태료를 감경할 수 있다.

【질서위반행위규제법 시행령】

제3조(사전통지 및 의견제출 등) ① 법 제16조 제1항에 따라 행정청이 과태료부과에 관하여 미리 통지하는 경우에는 다음 각 호의 사항을 모두 기재한 서면으로 하여야 한다.

1. 당사자의 성명(법인인 경우에는 명칭과 대표자의 성명)과 주소
2. 과태료 부과의 원인이 되는 사실, 과태료 금액 및 적용 법령
3. 과태료를 부과하는 행정청의 명칭과 주소
4. 당사자가 의견을 제출할 수 있다는 사실과 그 제출기한
5. 법 제18조에 따라 자진 납부하는 경우 과태료를 감경받을 수 있다는 사실(감경액이 결정된 경우에는 그 금액을 포함한다)

② 당사자는 제1항 제4호의 의견제출 기한 이내에 서면(전자문서를 포함한다) 또는 구두로 의견을 제출할 수 있고, 그 주장을 증명하기 위한 증거자료 등을 제출할 수 있다.

③ 행정청은 제2항에 따른 의견이 구두로 제출된 경우에는 진술자와 그 의견의 요지를 기록해 두어야 한다.

제5조(자진납부자에 대한 과태료 감경) 법 제18조 제1항에 따라 자진 납부하는 경우 감경할 수 있는 금액은 부과될 과태료의 100분의 20의 범위 이내로 한다.

(붙임 2)

제재내용 공개안

1. 금융회사명 : ㈜카카오페이

2. 제재조치일 : 2021. 5. 17.

3. 제재조치내용

제재대상	제재내용
기관	○ 과태료 부과 (6,960만원)
임직원	○ 주의 3명

4. 제재대상사실

가. 전자금융거래 안전성 확보의무 위반

(1) 클라우드컴퓨팅서비스 이용절차 등 수행 위반

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조 및 제14조의2 제1항부터 제3항, (舊)「전자금융감독규정」 제14조의2제1항부터 제3항에 의하면 전자금융업자는 비중요 정보처리시스템 지정 또는 클라우드컴퓨팅서비스(이하 '클라우드')를 이용하고자 하는 경우에 <비중요 정보처리시스템 지정절차> 또는 <클라우드 이용절차>를 수행하여야 하는데도,

○ 회사는 OOOO.O.O. ~ OOOO.O.O. 기간 중 OOOO 시스템을 OOO의 OOOO 클라우드 환경에서 사용하고 있었음에도 <비중요정보처리시스템 지정절차> 또는 <클라우드 이용절차>를 수행하지 않은 사실이 있음

< 관련법규 >
1.「전자금융거래법」 제21조제2항
2.「전자금융감독규정」 제7조, 제14조의2제1항, 제2항, 제3항 및 제9항
3. (舊)「전자금융감독규정」 제14조의2제1항, 제2항 및 제3항

(2) 내부 업무용시스템, 정보처리시스템 등의 망분리 이행 위반

□ 「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제7조 및 제15조제1항제3호에 의하면 전자금융업자는 내부통신망과 연결된 내부업무시스템을 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속을 금지하여야 하고,

「전자금융감독규정」 제15조제1항제5호에 의하면 회사의 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 하며,

클라우드 제공자의 전산실 내에 위치한 정보처리시스템에 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서도 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 하는데도,

① 회사는 OOOO.O.O. ~ OOOO.O.O. 기간 중 내부통신망에 연결된 본사 임직원의 업무단말기와 내부 업무용시스템에 대해 망분리 이행을 완료하지 않고 인터넷 등 외부통신망과 연결하여 운영하는 등 외부통신망과 분리·차단 및 접속을 금지하지 않고 운영하고 있으며

② 회사 전산실 내에 위치한 일부 정보처리시스템(OO·OO·OO 등의 업무처리 및 OO OOOOO OO 서버)에 대해서 인터넷(OO, OO, OOO, OOO 등의 이미지CDN, OO·OO OOOOO 등 홈페이지) 등 외부통신망과 물리적으로 분리하지 않고 연결하여 운영하는 한편,

회사 전산실의 정보처리시스템(OOOOOOOO)에 개발 목적으로 직접 접속하는 단말기에 대해서 인터넷 등 외부통신망과 물리적으로 분리하지 않고 연결하여 운영하고 있으며,

클라우드 제공자(OOO)의 정보처리시스템(OO, OO·OO·OO 설정관리콘솔)에 운영, 개발, 보안 목적으로 직접 접속하는 회사의 단말기에 대해서도 인터넷 등 외부통신망으로부터 물리적으로 분리하지 않고 연결하여 운영한 사실이 있음

< 관련법규 >
1.「전자금융거래법」 제21조제2항
2.「전자금융감독규정」 제7조, 제14조의2제8항, 제15조제1항 제3호, 제5호

(3) 홈페이지 등 공개용 웹서버 관리 대책 이행 위반

□ 「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제7조 및 제17조제1항제1호, 제3호, 제4호에 의하면 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 “DMZ구간”)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호하여야 하고,

공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한하여야 하며, DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니하여야 하는데도

(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 함)

① OOOO.O.O. ~ OOOO.O.O. 기간 중, OOO 클라우드의 공개용 웹서버(프로모션 이벤트 홈페이지)를 내부통신망과 분리하여 내부통신망과 외부통신망 사이의 독립된 통신망(DMZ구간)에 설치하지 아니하고 내부통신망에 설치하면서 웹 접근제어 수단(침입탐지시스템의 웹접근제어 규칙 등)으로 보호하지 않고 운영하고

② 회사 전산실 및 클라우드의 공개용 웹서버(OO, OOOO, OOOO 홈페이지 공개용 웹서버 등)에서 시험·개발도구(gcc, g++, make 등)의 사용을 제한하지 않고 운영하고 있으며

③ DMZ구간 내의 공개용 웹서버(OO·OOOO 홈페이지)의 거래로그에 이용자 OOOO 및 OOOOOO를 저장하여 관리하면서 암호화하지 않은 사실이 있음

< 관련법규 >
1.「전자금융거래법」제21조제2항
2.「전자금융감독규정」제7조, 제17조제1항제1호, 제3호, 제4호

(4) 프로그램 및 전산원장 관리통제 위반

□「전자금융거래법」제21조제2항 및「전자금융감독규정」제7조, 제27조제1항, 제2항, 제28조제2항, 제29조제7호, 제30조제5호에 의하면 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 변경내용의 정당여부에 대해 제3자 확인 등을 포함한 별도의 변경절차를 수립·운용하여야 하고 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 하여야 하며,

일괄작업(batch)의 수행을 위하여 책임자가 일괄작업 수행자의 주요업무 관련 행위를 모니터링하여야 하고 프로그램 반출, 실행 프로그램의 생성 및 운영시스템 등록을 전산자료 관리자 등 해당 프로그램 담당자 이외의 자가 수행하여야 하는데도

① OOOO.O.O. ~ OOOO.O.O. 기간 중 전산원장 변경내용의 정당 여부에 대해 내부감사 등 제3자의 승인없이 책임자의 승인만을 통해 변경을 실시하였고, 전산원장의 중요작업에 대한 책임자의 이중확인 및 일괄작업 수행자의 주요업무 관련 행위에 대한 책임자의 모니터링을 수행하지 않았으며,

② OOOO.O.O. ~ OOOO.O.O. 기간 중 프로그램 반출 및 운영시스템 등록을 해당 프로그램 담당 개발자가 직접 배포한 사실이 있음

< 관련법규 >

1.「전자금융거래법」제21조제2항
2.「전자금융감독규정」제7조, 제27조제1항, 제2항, 제28조제2항, 제29조 제7호, 제30조제5호

나. 전자금융거래 변경약관 게시 및 이용자 통지 위반

□「전자금융거래법」제24조제3항 및「전자금융감독규정」제40조제4항에 의하면 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 그 시행일 1월전에 해당 전자금융거래를 수행하는 전자적 장치에 게시하고 이용자에게 통지하여야 하는데도,

○ 회사는 OOOO.O.O. 'OOOOO 이용약관'(이하 '약관')을 제정한 이후 현재까지 총 O차례 약관을 변경하면서,

○ 변경된 약관을 전자적 장치에 지연 게시(O회)하거나, 통지기한 내에 이용자에게 통지하지 아니한(O회) 사실이 있음

< 관련법규 >

1.「전자금융거래법」제24조제3항

2.「전자금융감독규정」제40조제4항

다. 전자금융거래 약관 보고 위반

□「전자금융거래법」제25조제1항 및「전자금융감독규정」제41조제2항에 의하면 금융회사 또는 전자금융업자가 전자금융거래에 관한 약관을 제정하거나 변경하고자 하는 경우에는 미리 금융위원회에 보고하여야 하는데도,

○ 회사는 OOOO.O.O. 'OOOOO 이용약관'(이하 '약관')을 제정한 이후 현재까지 총 O차례 약관을 변경하면서

○ 제정 약관은 시행일(OOOO.O.O.)로부터 O일 후에 금융위원회에 지연하여 보고(OOOO.O.O.)하였고, 약관개정시행일이 OOOO.O.O. 등 약관(O건)은 금융위원회에 보고하지 않은 사실이 있음

< 관련법규 >

1.「전자금융거래법」제25조제1항

2.「전자금융감독규정」제41조제2항

< 의안 소관 부서명 >

	금융위원회	금융감독원
소관부서	전자금융과	디지털금융검사국
연 락 처	02-2100-2811	02-3145-7340