공 개

의안번호	제 243 호
의 결 연 월 일	2020. 7. 8. (제 13 차)

의결사항

㈜우리은행의 전자금융거래법 위반에 대한 과태료 부과처분안

금융위원회회의 안건

제 출 자	위 원 장 은 성 수
제출 연월일	2020. 7. 8.

1. 의결주문

㈜우리은행의 전자금융거래법 위반에 대한 과태료 부과처분안을 <별지>와 같이 의결하며「질서위반행위규제법」제16조 제1항에 따라 부여된 의견제출 기한 내에 제재조치 대상자가 과태료를 납부하지 아니하고 의견제출을 하지 아니하는 경우에는 <별지>의 처분안을 그대로 확정한다.

2. 제안이유

㈜우리은행에 대한 부문검사 결과 위법사항에 대하여 필요한 조치를 하려는 것임

3. 주요골자

㈜우리은행에 대한 부문검사 결과 '전자금융거래의 안전성 확보의무 위반' 및 '전자금융거래의 안전한 처리를 위한 선관주의 의무 위반' 사실이 확인되어「전자금융거래법」제51조에 따라 과태료를 부과하고자 함

4. 참고사항

가. 관계법규 : < 붙임 1 >

○「전자금융거래법」제21조(안전성의 확보의무) 제1항, 제2항, 제51조(과태료) 제1항 제1호

○「전자금융거래법 시행령」제33조(과태료의 부과기준), [별표3]

○「전자금융감독규정」제7조(전자금융거래 종류별 안전성 기준), 제8조(인력, 조직 및 예산) 제1항, 제17조(홈페이지 등 공개용 웹서버 관리대책) 제4항, 제29조(프로그램통제) 제6호

○「금융기관 검사 및 제재에 관한 규정」제20조(과징금 및 과태료의 부과) 제1항 및 제3항, [별표3] 과태료 부과기준

○ 「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)

나. 제재내용 공개안 < 붙임 2 >

다. 관계부서 협의

○ 제8차 제재심의위원회(2020.4.23.) 심의필

○ 제9차 제재심의위원회(2020.5.14.) 심의필

<별지>

㈜우리은행에 대하여 다음과 같이 조치한다.

- 다 음 -

1. 조치내용

□ 기관에 대한 조치

○ ㈜우리은행 : 과태료 8,000만원* 부과

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

- 조치사유 : 전자금융거래의 안전성 확보의무 위반(5,000만원)
전자금융거래의 안전성 확보의무 및 전자금융거래의 안전한 처리를 위한 선관주의 의무 위반(3,000만원)

- 법적근거 : 「전자금융거래법」 제51조 제1항 제1호
「전자금융거래법 시행령」 제33조, [별표3]

2. 조치사유

가. 차세대시스템 구축 부적정

□ 금융회사는 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설 및 정보기술부문 등에 관하여 금융위원회가 정하는 기준을 준수하여야 하고,

○ 금융위원회는 전자금융감독규정으로 그 기준을 정하여 금융회사로 하여금 인력, 조직 및 예산 부문, 건물, 전산실 등 시설부문, 단말기, 전산자료, 정보처리시스템 등 정보기술부문 등에 관하여 안전성을 갖추도록 의무를 부과하고 있음

1) 위 전자금융감독규정에 따라 금융회사는 전자금융업무와 관련된 정보처리시스템을 구축·운영하는 사업자인 전자금융보조업자와 제휴, 위탁 또는 외부주문(외부주문 등)에 관한 계약을 체결할 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사 내부의 조직과 인력을 갖추어야 하며,

2) 전자금융업무와 관련한 프로그램을 운영시스템에 적용하는 경우에는 처리하는 정보의 기밀성·무결성·가용성 등을 고려하여 충분한 테스트 후 실시하는 등 프로그램 등록·변경·폐기 절차를 수립·운영하여야 함

□ 그럼에도, ㈜우리은행은 차세대시스템 구축 사업을 추진하면서 다음 1)·2)와 같이 사업관리를 위한 충분한 인력·조직을 갖추지 아니하고, 처리정보의 무결성 등을 고려한 충분한 테스트를 실시하지 않는 등 그 의무를 위반하여,

차세대시스템 가동 이후 대외계 업무 중단(총 ♧♧시간 ♧♧분) 및 프로그램 오류 등으로 인한 약 ♠♠억원의 금전사고 등을 초래함으로써, 전자금융거래의 안전성과 신뢰성을 훼손한 사실이 있음

1) 우리은행은 ⊗⊗⊗⊗년 전산시스템 개발·운영 업무를 전산자회사(◈◈◈◈◈)에 일괄위탁(Total Outsourcing)하여 주로 계약관리 위주의 업무를 수행함으로 인해, 은행 IT인력의 대규모 IT사업 관리 경험이 부재하고, IT실무업무에 대한 전문성이 결여된 상황에서

차세대시스템 구축 사업을 추진함에 따라 외부주문 등 관련 사항을 자체적으로 통제하지 못하는 등 사업관리를 위한 충분한 인력·조직을 갖추어야 할 의무를 위반, 사업관리 부실을 야기

2) 차세대시스템의 운영시스템 적용에 있어서도 아래 가)·나)와 같이 장애발생 가능성이 높은 테스트유형을 누락하는 등 처리하는 정보의 기밀성·무결성·가용성을 고려한 충분한 테스트를 실시하여야 할 의무를 위반하여 테스트 단계에서 발견된 결함이 차세대시스템 가동 이후 동일하게 재발하는 등의 결과를 초래하였음

< 관련규정 >

「전자금융거래법」 제21조 제2항

「전자금융거래법」 제51조 제1항

「전자금융거래법 시행령」 제33조, [별표3]

「전자금융감독규정」 제7조, 제8조제1항제2호, 제29조제6호

「검사 및 제재에 관한 규정」 제20조 제1항, 제3항, [별표3]

나. 공개용 웹서버 해킹방지대책 불철저

□ 금융회사는 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설 및 정보기술부문 등에 관하여 금융위원회가 정하는 기준을 준수하여야 하고,

○ 금융위원회는 「전자금융 감독규정」으로 그 기준을 정하여 금융회사로 하여금 공개용 웹서버에 대한 관리대책을 수립·운용토록 의무를 부과하고 있음

□ 나아가, 비대면의 자동화된 방식으로 이루어지는 전자금융업무의 특성상 금융회사는 이용자 정보 등의 처리에 있어 고도의 자율성·독립성을 부여받고 있으므로

○ 그 보호 조치를 이행함에 있어서도, 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 함

□ 그런데, 우리은행은 다음 1)~3)과 같이 ◈◈◈◈시스템, ♣♣♣♣♣♣시스템, ◎◎◎◎◎◎◎◎◎시스템 등을 소홀히 운영함으로써

○ 2018.6.13.~28. 총 16일간 불상자의 ◆◆개 IP주소와 총 ♤,♤♤♤,♤♤♤개의 아이디(ID)로 우리은행 인터넷뱅킹 홈페이지에 총 ◇,◇◇◇,◇◇◇번 대량 부정 로그인이 시도된 사이버공격에서 그 중 로그인이 된 총 ○○,○○○개의 ID로 부정접속을 통해 고객의 인적사항, 거래내역 등에 관한 정보가 유출되었거나 유출이 의심되는 상황을 초래하게 하는 등

공개용 웹서버에 대한 관리대책을 충분히 갖추지 아니하였을 뿐만 아니라, 선량한 관리자로서 주의의무를 다하지 아니하여 전자금융거래의 안전성과 신뢰성을 훼손한 사실이 있음

1) 우선, ◈◈◈◈시스템 측면에서 볼 때, 우리은행은 위와 같은 사이버공격이 이루어진 기간 동안 ◈◈◈◈시스템을 운영하면서 검사기준일 최근 1년간(2017.11월~2018.10월) 은행 자체분석을 통해 사전에 등록된 임계치 변경이 약 ▣.▣%*에 불과하는 등 임계치(탐지기준) 조정이 미흡하였고

◈◈◈◈시스템을 차단모드가 아닌 탐지모드로 운영하는 등에 따라 위와 같은 사이버공격이 즉시 분석되지 않았을 뿐 아니라, 탐지된 부정접속 등 의심 내역에 대한 분석과 추가적인 사이버공격을 방지하기 위한 사후보완 조치가 필요함에도 불구하고, 이를 위한 분석**이나 사후보완 조치가 적시에 반영이 되지 않아 불상의 해커의 사이버공격에 장기간 노출되도록 하였음

2) 다음, ♣♣♣♣♣♣시스템의 측면에서 볼 때도, 우리은행은 위와 같은 사이버공격이 이루어진 기간 동안 ♣♣♣♣♣♣시스템을 운영하면서,

◈◈◈◈시스템을 통해 단시간에 시도되는 사이버공격을 차단함과 더불어, ♣♣♣♣♣♣시스템에 장기 보관된 데이터(통합 로그)를 통해 특정 기간 동안 이루어진 사이버공격 패턴 등을 분석하여 이상징후를 탐지하거나 그 분석 결과를 보안시스템 설정에 반영하는 등의 예방활동을 소홀히 하였음

3) 나아가, 우리은행은 위와 같은 사이버공격이 이루어진 기간 동안 ◎◎◎◎◎◎◎◎◎시스템를 운영하면서,

특정 IP주소가 특정 웹페이지에 일정한 조건 이상으로 접근하는 경우에 부정접속으로 탐지하게 되는 ◈◈◈◈시스템과는 달리, ◎◎◎◎◎◎◎◎◎시스템으로는 IP주소 접속이력 등을 활용하여 해커들이 사용하는 특정 단말기에서 인터넷뱅킹에 다수의 ID로 로그인하는 이상금융거래까지도 탐지할 수 있을 뿐만 아니라,

위와 같은 사이버공격 당시의 ◎◎◎◎◎◎◎◎◎시스템 기술 수준 등에 비추어 볼 때 특정 IP주소에서 특정 ID로 여러 번 로그인을 성공/실패하는 등의 정보를 활용하여 위와 같은 대량 부정접속(Credential Stuffing)을 충분히 탐지할 수 있었음에도 불구하고,

우리은행은 위 1)·2)와 같이 ◆◆◆◆시스템/♣♣♣♣♣♣시스템을 소홀히 운영한 사실 외에도 위와 같은 사이버공격이 이루어진 기간 동안 대량 부정접속 형태의 사이버공격을 탐지하거나 차단하기 위하여 ◎◎◎◎◎◎◎◎◎시스템을 가동하지 아니함으로써 전사적(全社的) 차원에서 개인신용정보를 보호해야 할 고객과의 신임관계를 저버린 사실이 있음.

< 관련규정 >
「전자금융거래법」 제21조 제1항, 제2항
「전자금융거래법」 제51조 제1항
「전자금융거래법 시행령」 제33조, [별표3]
「전자금융감독규정」 제7조, 제17조제4항
「검사 및 제재에 관한 규정」 제20조 제1항, 제3항, [별표3]

< 붙임 1 >

관계 법규

□ 「전자금융거래법」

제21조(안전성의 확보의무) ① 금융회사·전자금융업자 및 전자금융보조업자(이하 "금융회사등"이라 한다)는 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.

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)

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

1. 제21조제1항 또는 제2항을 위반하여 선량한 관리자로서의 주의를 다하지 아니하거나 금융위원회가 정하는 기준을 준수하지 아니한 자
2. (생략)

②~③ (생략)

④ 제1항부터 제3항까지의 규정에 따른 과태료는 금융위원회가 부과·징수한다.

□ 「전자금융거래법 시행령」

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

<별표3> 과태료의 부과기준(제33조 관련)

1. 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

가.~마. (생략)

바. 법 제21조제2항을 위반하여 금융위원회가 정하는 기준을 준수하지 않은 경우	법 제51조 제1항제1호	5,000 만원

사.~터. (생략)

□「전자금융감독규정」

제7조(전자금융거래 종류별 안전성 기준) 법 제21조제2항의 "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

제8조(인력, 조직 및 예산) ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 정보처리시스템 및 전자금융업무 관련 전담 조직을 확보할 것
2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것

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

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것
2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것
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)

② 금융회사 또는 전자금융업자는 공개용웹서버에 게재된 내용에 대하여 다음 각호의 사항을 준수하여야 한다.

1. 게시자료에 대한 사전 내부통제 실시
2. 무기명 또는 가명에 의한 게시 금지
3. 홈페이지에 자료를 게시하는 담당자의지정·운용
4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치

③ 삭제<2013.12.3>

④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응조치하여야 한다.

⑤ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

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

1. ~ 5. (생략)
6. 운영시스템 적용은 처리하는 정보의기밀성·무결성·가용성을 고려하여 충분한 테스트 및 관련 책임자 승인 후 실시할 것
7. ~ 10. (생략)

□ 「금융기관 검사 및 제재에 관한 규정」

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 부과 면제 사유에 해당한다고 판단하는 경우에는 부과 면제를 건의하여야 한다.

② (생략)

③ 제1항에 의하여 과징금 또는 과태료의 부과를 금융위에 건의하는 경우에는 <별표 2> 과징금 부과기준, <별표3>과태료 부과기준 및 <별표6> 업권별 과태료 부과기준에 의한다.

<별표3> 과태료 부과기준(2017.10.19. 개정)

1. (생략)

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. 하나의 행위가 2개 이상의 위반행위에 해당하는 경우에는 각 위반행위에 대하여 정한 과태료 중 가장 중한 과태료를 부과하며, 이를 제외하고 2개 이상의 위반행위가 경합하는 경우에는 각 위반행위에 대하여 정한 과태료를 각각 부과한다. 다만, 2개 이상의 동일한 종류의 위반행위에 대하여 과태료를 각각 부과하는 것이 합리적이지 않은 경우에는 그러하지 아니하다.

※ 2개 이상의 동일한 종류의 위반행위를 반복한 경우에는 반복된 행위의 시간적·장소적 근접성, 행위의사의 단일성, 침해된 법 규정의 동일성에 따라 행위의 동일성이 인정된다면 이를 하나의 행위로 평가할 수 있다.

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. 위반자에게 가중·감면사유가 있는 경우에는 위 예정금액을 가중·감면하여 과태료 부과금액을 산정한다.

마. 금융업관련법령 및 감독규정에서 업권별·위반행위 유형별로 별도의 기준을 정하는 경우 그 기준에 따른다. 이 경우 그 근거를 검사결과 처분안에 명시하여야 한다.

바. 과태료 부과에 있어 이 규정에서 정하고 있는 내용을 제외하고는 질서위반행위규제법에서 정하는 바를 따른다.

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 동일 위반행위가 언론(「방송법」에 따른 지상파방송사업자가 전국을 대상으로 행하는 방송 또는 「신문 등의 진흥에 관한 법률」에 따른 일반일간신문 중 서울에 발행소를 두고 전국을 대상으로 발행되는 둘 이상의 신문을 말한다. 이하 같다)에 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 동일 위반행위가 언론에 공표되어 당해 금융기관의 공신력을 실추시키거나 당해 금융기관이 신뢰를 상실하여 금융상품 해지 등이 초래된 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

나. 위반결과 및 동기에 따른 비율(이하 "예정비율"이라 한다)과 다른 비율을 적용할 사유(해당 사유가 가중 또는 감면사유와 중복되는 경우는 제외한다)가 있는 경우에는 예정비율을 달리 결정할 수 있다. 다만, 이 경우 그 사유를 검사결과 처분안에 명시하여야 한다.

다. 검사를 거부·방해 또는 기피한 경우에 대하여 과태료를 부과할 때에는 위반결과를 '중대'로 본다.

4.~6. (생략)

□「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 의견 제출이 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.

② 당사자가 제1항에 따라 감경된 과태료를 납부한 경우에는 해당 질서위반행위에 대한 과태료 부과 및 징수절차는 종료한다.

□「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 : ㈜우리은행

2. 제재조치일 : 2020. 7. 8.

3. 제재조치내용

제재대상	제재내용
기관	○ 기관경고 ○ 과태료 부과(8,000만원) ○ 자율처리필요사항 1건
임직원 (6명)	○ 퇴직자 위법·부당사항(문책경고 상당) 1명 ○ 퇴직자 위법·부당사항(주의적경고 상당) 1명 ○ 퇴직자 위법·부당사항(정직3월 상당) 2명 ○ 감봉3월 1명 ○ 퇴직자 위법·부당사항(주의 상당) 1명

4. 제재대상사실

가. 차세대시스템 구축 부적정

□ 금융회사는 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설 및 정보기술부문 등에 관하여 금융위원회가 정하는 기준을 준수하여야 하고,

○ 금융위원회는 전자금융감독규정으로 그 기준을 정하여 금융회사로 하여금 인력, 조직 및 예산 부문, 건물, 전산실 등 시설부문, 단말기, 전산자료, 정보처리시스템 등 정보기술부문 등에 관하여 안전성을 갖추도록 의무를 부과하고 있음

1) 위 전자금융감독규정에 따라 금융회사는 전자금융업무와 관련된 정보처리시스템을 구축·운영하는 사업자인 전자금융보조업자와 제휴, 위탁 또는 외부주문(외부주문 등)에 관한 계약을 체결할 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사 내부의 조직과 인력을 갖추어야 하며,

2) 전자금융업무와 관련한 프로그램을 운영시스템에 적용하는 경우에는 처리하는 정보의 기밀성·무결성·가용성 등을 고려하여 충분한 테스트 후 실시하는 등 프로그램 등록·변경·폐기 절차를 수립·운영하여야 함

□ 그럼에도, ㈜우리은행은 차세대시스템 구축 사업을 추진하면서 다음 1)·2)와 같이 사업관리를 위한 충분한 인력·조직을 갖추지 아니하고, 처리정보의 무결성 등을 고려한 충분한 테스트를 실시하지 않는 등 그 의무를 위반하여,

차세대시스템 가동 이후 대외계 업무 중단(총 ♧♧시간 ♧♧분) 및 프로그램 오류 등으로 인한 약 ♠♠억원의 금전사고 등을 초래함으로써, 전자금융거래의 안전성과 신뢰성을 훼손한 사실이 있음

1) 우리은행은 ⊗⊗⊗⊗년 전산시스템 개발·운영 업무를 전산자회사(◈◈◈◈◈)에 일괄위탁(Total Outsourcing)하여 주로 계약관리 위주의 업무를 수행함으로 인해, 은행 IT인력의 대규모 IT사업 관리경험이 부재하고, IT실무업무에 대한 전문성이 결여된 상황에서

   차세대시스템 구축 사업을 추진함에 따라 외부주문 등 관련 사항을 자체적으로 통제하지 못하는 등 사업관리를 위한 충분한 인력·조직을 갖추어야 할 의무를 위반, 사업관리 부실을 야기

2) 차세대시스템의 운영시스템 적용에 있어서도 아래 가)·나)와 같이 장애발생 가능성이 높은 테스트유형을 누락하는 등 처리하는 정보의 기밀성·무결성·가용성을 고려한 충분한 테스트를 실시하여야 할 의무를 위반하여 테스트 단계에서 발견된 결함이 차세대시스템 가동 이후 동일하게 재발하는 등의 결과를 초래하였음

< 관련규정 >

「전자금융거래법」 제21조 제2항

「전자금융거래법」 제51조 제1항

「전자금융거래법 시행령」 제33조, [별표3]

「전자금융감독규정」 제7조, 제8조제1항제2호, 제29조제6호

「검사 및 제재에 관한 규정」 제20조 제1항, 제3항, [별표3]

나. 공개용 웹서버 해킹방지대책 불철저

□ 금융회사는 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설 및 정보기술부문 등에 관하여 금융위원회가 정하는 기준을 준수하여야 하고,

○ 금융위원회는 「전자금융 감독규정」으로 그 기준을 정하여 금융회사로 하여금 공개용 웹서버에 대한 관리대책을 수립·운용토록 의무를 부과하고 있음

□ 나아가, 비대면의 자동화된 방식으로 이루어지는 전자금융업무의 특성상 금융회사는 이용자 정보 등의 처리에 있어 고도의 자율성·독립성을 부여받고 있으므로

○ 그 보호 조치를 이행함에 있어서도, 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 함

□ 그런데, 우리은행은 다음 1)~3)과 같이 ◈◈◈◈시스템, ♣♣♣♣♣♣시스템, ◎◎◎◎◎◎◎◎◎시스템 등을 소홀히 운영함으로써

○ 2018.6.13.~28. 총 16일간 불상자의 ◆◆개 IP주소와 총 ♤,♤♤♤,♤♤♤개의 아이디(ID)로 우리은행 인터넷뱅킹 홈페이지에 총 ◇,◇◇◇,◇◇◇번 대량 부정 로그인이 시도된 사이버공격에서 그 중 로그인이 된 총 ○○,○○○개의 ID로 부정접속을 통해 고객의 인적사항, 거래내역 등에 관한 정보가 유출되었거나 유출이 의심되는 상황을 초래하게 하는 등

공개용 웹서버에 대한 관리대책을 충분히 갖추지 아니하였을 뿐만 아니라, 선량한 관리자로서 주의의무를 다하지 아니하여 전자금융거래의 안전성과 신뢰성을 훼손한 사실이 있음

1) 우선, ◈◈◈◈시스템 측면에서 볼 때, 우리은행은 위와 같은 사이버공격이 이루어진 기간 동안 ◈◈◈◈시스템을 운영하면서 검사기준일 최근 1년간(2017.11월~2018.10월) 은행 자체분석을 통해 사전에 등록된 임계치 변경이 약 ▣.▣%*에 불과하는 등 임계치(탐지기준) 조정이 미흡하였고

◈◈◈◈시스템을 차단모드가 아닌 탐지모드로 운영하는 등에 따라 위와 같은 사이버공격이 즉시 분석되지 않았을 뿐 아니라, 탐지된 부정접속 등 의심 내역에 대한 분석과 추가적인 사이버공격을 방지하기 위한 사후보완 조치가 필요함에도 불구하고, 이를 위한 분석**이나 사후보완 조치가 적시에 반영이 되지 않아 불상의 해커의 사이버공격에 장기간 노출되도록 하였음

2) 다음, ♣♣♣♣♣♣시스템의 측면에서 볼 때도, 우리은행은 위와 같은 사이버공격이 이루어진 기간 동안 ♣♣♣♣♣♣시스템을 운영하면서,

◈◈◈◈시스템을 통해 단시간에 시도되는 사이버공격을 차단함과 더불어, ♣♣♣♣♣♣시스템에 장기 보관된 데이터(통합 로그)를 통해 특정 기간 동안 이루어진 사이버공격 패턴 등을 분석하여 이상징후를 탐지하거나 그 분석 결과를 보안시스템 설정에 반영하는 등의 예방활동을 소홀히 하였음

3) 나아가, 우리은행은 위와 같은 사이버공격이 이루어진 기간 동안 ◎◎◎◎◎◎◎◎◎시스템을 운영하면서,

특정 IP주소가 특정 웹페이지에 일정한 조건 이상으로 접근하는 경우에 부정접속으로 탐지하게 되는 ◈◈◈◈시스템과는 달리, ◎◎◎◎◎◎◎◎◎시스템으로는 IP주소 접속이력 등을 활용하여 해커들이 사용하는 특정 단말기에서 인터넷뱅킹에 다수의 ID로 로그인하는 이상금융거래까지도 탐지할 수 있을 뿐만 아니라,

위와 같은 사이버공격 당시의 ◎◎◎◎◎◎◎◎◎시스템 기술 수준 등에 비추어 볼 때 특정 IP주소에서 특정 ID로 여러 번 로그인을 성공/실패하는 등의 정보를 활용하여 위와 같은 대량 부정접속(Credential Stuffing)을 충분히 탐지할 수 있었음에도 불구하고,

우리은행은 위 1)·2)와 같이 ◆◆◆◆시스템/♣♣♣♣♣♣시스템을 소홀히 운영한 사실 외에도 위와 같은 사이버공격이 이루어진 기간 동안 대량 부정접속 형태의 사이버공격을 탐지하거나 차단하기 위하여 ◎◎◎◎◎◎◎◎◎시스템을 가동하지 아니함으로써 전사적(全社的) 차원에서 개인신용정보를 보호해야 할 고객과의 신임관계를 저버린 사실이 있음.

< 관련규정 >
「전자금융거래법」 제21조 제1항, 제2항
「전자금융거래법」 제51조 제1항
「전자금융거래법 시행령」 제33조, [별표3]
「전자금융감독규정」 제7조, 제17조제4항
「검사 및 제재에 관한 규정」 제20조 제1항, 제3항, [별표3]

< 의안 소관 부서명 >

	금융위원회	금융감독원
소관부서	전자금융과	IT·핀테크전략국
연 락 처	02-2100-2811	02-3145-7330