공 개

의안번호	제 223 호
의 결 연 월 일	2020. 6. 24. (제 12 차)

의결사항

한화투자증권㈜에 대한 부문검사 결과 조치안

금융위원회회의 안건

제 출 자	위원장 은 성 수
제출 연월일	2020. 6. 24.

1. 의결주문

한화투자증권㈜에 대한 부문검사 결과 조치안을 <별지>와 같이 의결하며 「질서위반행위규제법」 제16조 제1항에 따라 부여된 의견제출기한 내에 제재조치 대상자가 과태료를 납부하지 아니하고 의견제출을 하지 아니하는 경우에는 <별지>의 조치안을 그대로 확정함

2. 제안이유

2019. 5. 13. ~ 2019. 5. 24. 기간 중 실시한 한화투자증권㈜에 대한 부문검사 결과 적발된 위규행위에 대하여 필요한 조치를 하려는 것임

* 검사대상기간 : 2016. 4. 1. ~ 2019. 5. 24.

3. 주요골자

한화투자증권㈜에 대한 부문검사 결과 '전자금융거래의 안전성 확보의무 위반' 및 '신용정보전산시스템 보안대책 의무 위반'이 적발되어 「전자금융거래법」 제51조 및 「신용정보의 이용 및 보호에 관한 법률」 제52조에 따라 과태료를 부과하고자 함

4. 참고사항

가. 금융감독원장이 안건 상정을 요청한 사항임

나. 관계법규 : <붙임 1>

다. 제재내용 공개안 : <붙임 2>

라. 관계부서 협의

○ 제10차 제재심의위원회(2020.5.22.) 심의필

<별지>

한화투자증권㈜에 대하여 다음과 같이 조치한다.

- 다 음 -

1. 조치내용

□ 기관에 대한 조치

○ 한화투자증권㈜ : 과태료 54백만원 부과

- 조치사유

· 전자금융거래의 안전성 확보의무 위반 : 30백만원
· 신용정보전산시스템 보안대책 의무 위반 : 24백만원

2. 조치사유

가. 전자금융거래의 안전성 확보의무 위반

⑴ 정보처리시스템과 직접 접속하는 단말기에 대한 망분리 미이행

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조 및 제15조제1항제5호에 의하면 금융회사는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 하는데도

한화투자증권㈜은 검사착수일 현재 정보처리시스템과 직접 접속하는 단말기 ◎◎대에 대해 인터넷 등 외부통신망으로부터 물리적으로 분리하지 않고 운영한 사실이 있음

⑵ 내부사용자 비밀번호 관리 부적정

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조, 제32조제2호에 의하면 금융회사는 내부사용자의 비밀번호 유출을 방지하기 위하여 비밀번호 관리정책*을 시스템에 반영하고 시스템마다 관리자 비밀번호를 다르게 부여하여야 하는데도

* 이용자 식별부호(아이디)를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정

한화투자증권㈜은 검사착수일 현재 데이터베이스 서버 ◇◇대의 관리자 비밀번호를 8자리 미만으로 설정하거나 특수문자를 포함하지 아니하거나 관리자 비밀번호를 동일하게 부여하는 등 비밀번호 관리를 소홀히 한 사실이 있음

⑶ 개발용 데이터베이스 운영·통제 미준수

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조 및 제13조제1항제10호에 의하면 금융회사는 전산자료의 유출, 파괴 등을 방지하기 위해 테스트 시 이용자 정보 사용이 금지됨에도

한화투자증권㈜은 뱅킹 인터넷지로 수납업무 개발 및 테스트를 위해 검사착수일 현재 업무계 운영 데이터베이스에 저장중인 이용자정보 △△△건(중복제외)을 사용한 사실이 있음

나. 신용정보전산시스템 보안대책 의무 위반

□ 「신용정보의 이용 및 보호에 관한 법률」 제19조제1항, 동법 시행령 제16조제2항, 「신용정보업감독규정」 제20조 및 별표3에 의하면 금융회사는 내부망에 주민등록번호를 저장하는 경우에는 개인신용정보처리시스템에 적용되고 있는 개인신용정보 보호를 위한 수단과 개인신용정보 유출시 신용정보주체의 권익을 해할 가능성 및 그 위험의 정도를 분석(이하 '위험도 분석')하여 암호화 적용여부 및 적용범위를 정하여야 하고,

○ 신용정보관리·보호인은 신용정보보호 관련 법령 및 규정 준수 여부를 점검하여야 하는데도,

⑴ 한화투자증권㈜은 검사착수일 현재 내부망에 있는 데이터베이스 내 '□□□' 등 ◉◉개 테이블에 저장된 주민등록번호 ◇◇◇건(중복제외)에 대해 위험도 분석을 실시하지 아니한 채 암호화하지 않았으며,

⑵ 신용정보관리·보호인은 내부망에 있는 주민등록번호의 암호화 여부에 대한 점검업무를 소홀히 하여 상기 주민등록번호에 대한 암호화 미적용 사실을 발견하지 못하였음

< 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)

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	5,000만원

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

제13조(전산자료 보호대책) ① 금융회사는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.

1. ~ 9. (생략)
10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지 (다만, 법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 테스트 시 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)
11. ~ 14. (생략)

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

1. ~ 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.)

제32조(내부사용자 비밀번호 관리) 금융회사는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. (생략)
2. 비밀번호는 다음 각 목의 사항을 준수할 것
   가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경
   나. (생략)
   다. 시스템마다 관리자 비밀번호를 다르게 부여
3. (생략)

□ 신용정보의 이용 및 보호에 관한 법률

제19조(신용정보전산시스템의 안전보호) ① 신용정보회사 등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.

제52조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

1. ~ 2. (생략)
3. 제19조를 위반한 자
4. ~ 8. (생략)

□ 신용정보의 이용 및 보호에 관한 법률 시행령

제16조(기술적·물리적·관리적 보안대책의 수립) ① 법 제19조제1항에 따라 신용정보회사 등은 신용정보전산시스템의 안전보호를 위하여 다음 각 호의 사항이 포함된 기술적·물리적·관리적 보안대책을 세워야 한다.

② 금융위원회는 제1항 각 호에 따른 사항의 구체적인 내용을 정하여 고시할 수 있다.

제38조(위반행위별 과태료의 부과기준)

법 52조 제1항부터 제4항까지의 규정에 따른 과태료의 부과기준은 별표4와 같다.

<별표 4> 과태료의 부과기준(제38조 관련)

1. 일반기준

가. ~ 나. (생략)

다. 금융위원회는 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 금액의 2분의 1의 범위에서 그 금액을 늘릴 수 있다. 다만, 법 제52조제1항부터 제4항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

1) (생략)
2) 법 위반상태의 기간이 6개월 이상인 경우
3) (생략)

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	금액
파. 법 제19조제1항을 위반하여 기술적·물리적·관리적 보안대책을 수립·시행하지 않은 경우	법 제52조 제1항제3호	4,000

□ 신용정보업감독규정

제20조 (기술적·물리적·관리적 보안대책) 영 제16조제2항에 따라 신용정보회사등이 마련해야 할 기술적·물리적·관리적 보안대책의 구체적인 사항은 별표3과 같다.

<별표 3> 기술적·물리적·관리적 보안대책 마련 기준(제20조 관련)

Ⅰ. (생략)

Ⅱ. 기술적 · 물리적 보안대책

1. ~ 2. (생략)

3. 개인신용정보의 암호화

① ~ ③ (생략)

④ 신용정보회사등은 다음 각 호의 기준에 따라 주민등록번호의 암호화 등의 조치를 취하여야 함

1. ~ 2. (생략)

3. 신용정보회사 등이 내부망에 주민등록번호를 저장하는 경우에는 다음 각목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있음

나. 그 밖의 신용정보회사등의 경우에는 개인신용정보처리시스템에 적용되고 있는 개인신용정보 보호를 위한 수단과 개인신용정보 유출시 신용정보주체의 권익을 해할 가능성 및 그 위험의 정도를 분석한 결과

Ⅲ. 관리적 보안대책

1. 신용정보관리 · 보호인

① 신용정보관리 · 보호인은 다음 각 호의 업무를 담당한다.

1. ~ 5. (생략)

6. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검

□ 「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 조치안에 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. ~ 다. (생략)

4.~6. (생략)

< 붙임 2 >

제재내용 공개안

1. 금융회사명 : 한화투자증권㈜

2. 제재조치일 : 2020. 7. 2.

3. 제재조치내용

제재대상	제재내용
기관	과태료 54백만원 부과 자율처리 필요사항 통보
임원	주의 1명

4. 제재대상사실

가. 전자금융거래의 안전성 확보의무 위반

(1) 정보처리시스템과 직접 접속하는 단말기에 대한 망분리 미이행

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조 및 제15조제1항제5호에 의하면 금융회사는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 하는데도

한화투자증권㈜은 검사착수일 현재 정보처리시스템과 직접 접속하는 단말기 ◎◎대에 대해 인터넷 등 외부통신망으로부터 물리적으로 분리하지 않고 운영한 사실이 있음

⑵ **내부사용자 비밀번호 관리 부적정**

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조, 제32조제2호에 의하면 금융회사는 내부사용자의 비밀번호 유출을 방지하기 위하여 비밀번호 관리정책을 시스템에 반영하고 시스템마다 관리자 비밀번호를 다르게 부여하여야 하는데도

한화투자증권㈜은 검사착수일 현재 데이터베이스 서버 ◇◇대의 관리자 비밀번호를 8자리 미만으로 설정하거나 특수문자를 포함하지 아니하거나 관리자 비밀번호를 동일하게 부여하는 등 비밀번호 관리를 소홀히 한 사실이 있음

⑶ **개발용 데이터베이스 운영·통제 미준수**

□ 「전자금융거래법」 제21조제2항, 「전자금융감독규정」 제7조 및 제13조제1항제10호에 의하면 금융회사는 전산자료의 유출, 파괴 등을 방지하기 위해 테스트 시 이용자 정보 사용이 금지됨에도

한화투자증권㈜은 뱅킹 인터넷지로 수납업무 개발 및 테스트를 위해 검사착수일 현재 업무계 운영 데이터베이스에 저장중인 이용자정보 △△△건을 사용한 사실이 있음

나. 신용정보전산시스템 보안대책 의무 위반

□ 「신용정보의 이용 및 보호에 관한 법률」 제19조제1항, 동법 시행령 제16조제2항, 「신용정보업감독규정」 제20조 및 별표3에 의하면 금융회사는 내부망에 주민등록번호를 저장하는 경우에는 개인신용정보처리시스템에 적용되고 있는 개인신용정보 보호를 위한 수단과 개인신용정보 유출시 신용정보주체의 권익을 해할 가능성 및 그 위험의 정도를 분석(이하 '위험도 분석')하여 암호화 적용여부 및 적용범위를 정하여야 하고,

○ 신용정보관리·보호인은 신용정보보호 관련 법령 및 규정 준수 여부를 점검하여야 하는데도,

⑴ 한화투자증권㈜은 검사착수일 현재 내부망에 있는 데이터베이스 내 '□□□' 등 ◉◉개 테이블에 저장된 주민등록번호 ◇◇◇건에 대해 위험도 분석을 실시하지 아니한 채 암호화하지 않았으며,

⑵ 신용정보관리·보호인은 내부망에 있는 주민등록번호의 암호화 여부에 대한 점검업무를 소홀히 하여 상기 주민등록번호에 대한 암호화 미적용 사실을 발견하지 못하였음

< 의안 소관 부서명 >

	금융위원회	금융감독원
소관부서	전자금융과	IT·핀테크전략국
연 락 처	02-2100-2811	02-3145-7430