

공 개



의안번호	제 118 호	의 결 사 항
의 결 연 월 일	2020. 4. 1. (제 6 차)	

SK증권(주)에 대한 부문검사 결과 조치안

금융위원회회의 안건

제 출 자	위원장 은 성 수
제출 연월일	2020. 4. 1.

## 1. 의결주문

SK증권(주)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. 7. 8. ~ 2019. 7. 16. 기간 중 실시한 SK증권(주)에 대한 부문검사 결과 적발된 위규행위에 대하여 필요한 조치를 하려는 것임

\* 검사대상기간 : 2017. 4. 7. ~ 2019. 7. 16.

## 3. 주요골자

신용정보전산시스템 내 보관 중인 고객 주민등록번호에 대해 위험도 분석 실시없이 암호화하지 않는 등 신용정보전산시스템의 보안대책 위규 사항에 대한 과태료 부과 조치를 취하고자 함

## 4. 참고사항

가. 금융감독원장이 안전 상정을 요청한 사항임

나. 관계법규 : <붙임 1>

다. 제재내용 공개안 : <붙임 2>

라. 관계부서 협의

○ 제6차 제재심의위원회(2020.3.12.) 심의필

<별지>

SK증권(주)에 대하여 다음과 같이 조치한다.

- 다 음 -

## 1. 조치내용

### □ 기관에 대한 조치

○ SK증권(주) : 과태료 24백만원 부과

- 조치사유

· 신용정보전산시스템 보안대책 의무 위반: 24백만원

## 2. 조치사유

### 가. 신용정보전산시스템 보안대책 의무 위반

□ 「신용정보의 이용 및 보호에 관한 법률」(이하 「신용정보법」) 제19조 제1항, 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,

(가) SK증권(주)은 검사착수일 현재 내부망에 있는 데이터베이스(○○○○\*)의 '○○○' 테이블에 대해 위험도 분석을 실시하지 아니한 채 동 테이블에 보관 중인 주민등록번호 000건(중복제외)을 암호화하지 않았으며,

\* 고객정보, 주식거래내역, 출금이체 내역 등 전산원장을 보관하는 계정계 업무 데이터베이스와 전산원장을 이용하여 고객별 맞춤형 정보제공 또는 마케팅 등 내부업무에 활용하기 위한 정보를 함께 보관하고 있는 데이터베이스

‘△△△’ 및 ‘◇◇◇◇’ 테이블에 대하여는 ○○개 점검항목으로 위험도 분석을 실시\*하고 동 테이블에 보관중인 주민등록번호는 암호화가 불필요한 것으로 정하였으나,

\* 데이터베이스 접속이 가능한 관리자 PC에 대한 인터넷 접속가능한 내부망의 네트워크 분리 여부 등 ●개 점검항목 중 ‘해당 없음’ 항목 ◆개를 제외한 ▲개 항목은 모두 충족한 것으로 분석

위험도 분석 이후 일부 점검항목이 위험도 분석 당시 점검기준에 부합되지 않아\* 위험도 분석 재실시를 통해 암호화 적용 여부 등을 정하여야 하는데도, 위험도 분석 재실시 없이 해당 테이블에 보관 중인 주민등록번호 ○○○건 (중복제외)을 암호화하지 않고 보관한 사실이 있음

\* 검사착수일 현재, 데이터베이스 접속이 가능한 관리자 PC에서 인터넷 접속이 가능

데이터베이스별 주민등록번호 미암호화 현황

데이터베이스명	테이블 용도 (테이블 명)	미암호화 건수
○○○	대량매일 발송(□□□)	○○○
	출금이체 원장 (△△△)	○○○
	출금이체 보조원장 (▽▽▽)	○○○
합 계		○○○

(나) 신용정보관리·보호인은 검사대상 기간 중 총 ○회(○○○, ○○○)에 걸쳐 신용정보 관련 법규 준수여부에 대한 점검을 실시했음에도, 상기 데이터베이스 내 위험도 분석 미실시 및 고객 주민등록번호에 대한 암호화 미적용 사실을 발견하지 못하는 등 기술적·물리적·관리적 보안대책의 준수여부에 대한 점검업무를 소홀히 한 사실이 있음

#### < 관계 법규 >

- 「신용정보의 이용 및 보호에 관한 법률」 제19조 제1항

## 관계 법규

### 【 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.
3. 제19조를 위반한 자

### 【 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 함
- ② 금융위원회는 제1항 각 호에 따른 사항의 구체적인 내용을 정하여 고시할 수 있음

### 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)

##### (Ⅱ. 기술적·물리적 보안대책)

3. 개인신용정보의 암호화 ④ 신용정보회사등은 다음 각 호의 기준에 따라 주민등록번호의 암호화 등의 조치를 취하여야 함
  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 있는개인 신용정보 보호를 위한 수단과 개인신용정보 유출시 신용정보주체의 권익을 해할 가능성 및 그 위험의 정도를 분석한 결과

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

##### (Ⅲ. 관리적 보안대책)

1. 신용정보관리·보호인 ① 신용정보관리·보호인은 다음 각 호의 업무를 담당한다.
  6. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검

### <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. 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. (생략)

#### 3. 예정금액의 산정

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

위반결과 \ 동기	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 기본적인 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



## 제재내용 공개안

1. 금융회사명 : SK증권(주)

2. 제재조치일 : 2020. 4. 3.

3. 제재조치내용

제재대상	제재내용
기관	과태료 24백만원 부과
임원	주의 2명

4. 제재대상사실

### (1) 신용정보전산시스템 보안대책 의무 위반

- ☐ 「신용정보의 이용 및 보호에 관한 법률」(이하 「신용정보법」) 제19조 제1항, 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,

(가) SK증권(주)은 검사착수일 현재 내부망에 있는 데이터베이스의 ‘○○○○’ 테이블에 대해 위험도 분석을 실시하지 아니한 채 동 테이블에 보관 중인 주민등록번호 ○○○건을 암호화하지 않았으며,

‘△△△’ 및 ‘◇◇◇◇’ 테이블에 대하여는 〇〇개 점검항목으로 위험도 분석을 실시하고 동 테이블에 보관중인 주민등록번호는 암호화가 불필요한 것으로 정하였으나,

위험도 분석 이후 일부 점검항목이 위험도 분석 당시 점검기준에 부합되지 않아 위험도 분석 재실시를 통해 암호화 적용 여부 등을 정하여야 하는데도, 위험도 분석 재실시 없이 해당 테이블에 보관 중인 주민등록번호 〇〇〇건을 암호화하지 않고 보관한 사실이 있음

(나) 신용정보관리·보호인은 검사대상 기간 중 총 〇회에 걸쳐 신용정보 관련 법규 준수여부에 대한 점검을 실시했음에도, 상기 데이터베이스 내 위험도 분석 미실시 및 고객 주민등록번호에 대한 암호화 미적용 사실을 발견하지 못하는 등 기술적·물리적·관리적 보안대책의 준수여부에 대한 점검업무를 소홀히 한 사실이 있음

#### < 관계 법규 >

- 「신용정보의 이용 및 보호에 관한 법률」 제19조 제1항

< 의안 소관 부서명 >

	금융위원회	금융감독원
소관부서	금융데이터정책과	IT·핀테크전략국
연 락 처	02-2100-2625	02-3145-7430