금융위원회

의결 제2022-241호

1. 조치대상자의 인적사항

제재대상	내용(회사명, 성명 등)
기 관	㈜하나은행
직 원	前 부장 ○○○, 前 부장 □□□

2. 조치내용

□ 기관에 대한 조치

◦ 「보험업법」상 '보험모집자격이 없는 직원에 대한 보험 부당모집 위반', 「퇴직급여법」상 '개인형퇴직연금제도 가입자에 대한 교육 미실시', 「전자금융거래법」상 '전자금융거래의 안정성 확보의무' 위반으로 과태료 3억 7,600만원* 부과

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

□ 임직원에 대한 조치

◦ 「은행법」상 '국외점포에 대한 현지 감독기관 제재 보고의무 위반'에 대해 前 부장 ○○○에게 과태료 150만원, 前 부장 □□□에게 과태료 60만원 부과조치

3. 조치이유

가. 지적사항

□ 기관

1. 보험모집자격이 없는 직원에 의한 보험 부당모집

◦「보험업법」 제100조 제1항 제6호 등에 의하면 금융기관보험대리점 등은 점포별로 2명의 범위 내에서 정한 보험 모집 종사자 외의 임직원에게 보험상품의 구입에 대한 상담 또는 소개를 하게 하여서는 아니 되는데도,

- ㈜하나은행(★★★지점 등 5개 영업점)은 2018.4.18.~2020.5.25. 기간 중 점포별로 정한 보험 모집 종사자 외의 직원 4명(PB)이 본인의 전담고객* 12명에게 (△)△△생명 △△△△△△△저축보험 등 ◇◇건(보험료 ▽▽.▽억원, 수수료 ■■.■백만원)의 보험상품 구입에 대한 상담 또는 소개 행위를 한 사실이 있음

* PB의 전담고객에 대한 보험판매 실적은 PB 본인의 KPI에 반영

2. 개인형퇴직연금제도 가입자에 대한 교육 미실시

◦「근로자퇴직급여 보장법」(이하 “퇴직급여법”이라 함) 제33조 제5항 등에 의하면 개인형퇴직연금제도를 운영하는 퇴직연금사업자는 해당 사업의 퇴직연금제도 운영 상황 등 법정 사항에 대하여 매년 1회 이상 가입자에게 교육을 실시하여야 하는데도,

- ㈜하나은행(▲▲▲▲▲▲부)은 2018.7.14.~2020.4.16. 기간 중 개인형 퇴직연금제도 가입자 ☆☆,☆☆☆명에 대하여 교육을 실시하지 아니한 사실이 있음*

* 은행의 신(新)주소(도로명 주소) 체계 전환 과정에서 퇴직연금 전산 시스템의 오류가 발생하여 개인형퇴직연금제도 가입자에 대한 교육자료가 잘못된 주소지로 발송

3. 전자금융거래의 안전성 확보의무 위반

1) 스마트뱅킹시스템 관련 전자금융거래 무결성 검증 방법 제공 위반

◦「전자금융거래법」 제21조 제2항 및 「전자금융감독규정」 제34조 제5호에 의하면 금융회사는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래 프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공하여야 하는데도,

- ㈜하나은행(■■■■■■■■■■■■ ■ ■■■그룹, 이하 '■■■그룹')은 2016.6.7. 스마트뱅킹시스템(이하 '◁◁◁◁')을 구축하면서, 거래 전문의 이중처리(이하 '중복이체')를 방지하기 위한 무결성 검증방법 중 일부*를 전자금융거래에 제공하지 아니한 채 운영하였고,

* 이용자의 중복클릭으로 인한 중복이체 방지대책은 제공하였으나, 모바일 무선통신망 환경변화에 따른 IP변경 등 통신망이나 시스템 문제로 인한 중복이체 방지대책은 미제공

- 2016.7.29.~2020.11.6. 기간 중 ◁◁◁◁를 통한 이체거래 시, 이용자가 의도하지 않은 다수*의 중복이체가 실행되어 총 ◎,◎◎◎건(◎,◎◎◎명), ◐◐◐,◐◐◐,◐◐◐원의 중복이체 거래가 발생한 사실이 있음**

* 이용자의 거래지시 내용이 2~5회 범위 내에서 중복 이체됨

** 2020.11.6. 중복이체 방어로직 적용 후 추가 사고 미발생

2) 스마트뱅킹시스템 성능관리 위반

◦「전자금융거래법」 제21조 제2항 및 「전자금융감독규정」 제25조에 의하면 금융회사는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 하는데도,

- ㈜하나은행(▣▣▣그룹)은 스마트뱅킹(◁◁◁◁) 구축일*(2016.6.7.) 이후 장애사고 발생일(2019.9.25.)까지 신규 가입자 수 및 거래량이 꾸준히 증가**하였음에도 시스템 부하 성능을 확인***할 수 있는 추이 분석을 실시하지 않아

* 접속자 수 또는 거래량 급증에 따른 시스템 과부하를 방지하기 위해서는 부하 성능을 확인해야 하는데, ◁◁◁◁ 구축당시 실시(2016.3.7.~5.12.)한 부하 성능 테스트 결과 ◁◁◁◁의 1초당 처리 가능한 최대 거래량(TPS)은 768 수준

** 신규 가입자 수 71.1% 증가(603만명→1,032만명), 총 거래량 92.1% 증가(432백만건 → 830백만건)

*** 초당 최대 거래량(TPS), 응답시간, 피크타임 기준 동시접속자 수 등

- ◁◁◁◁ 구축 이후 장애예방 및 시스템 성능의 최적화를 위해 중앙처리장치(CPU)를 추가적으로 증설하지 않고* 운영함으로써

* 구축시점 대비 2019.5월~10월 기간 중 초당 거래량은 35%(1,033 TPS) 는 약 70% (6,886~11,688건) 증가하는 등 중앙처리장치(CPU)의 추가 증설이 필요한 상황이었음

- 2019.9.25. 10:55~16:17 기간 중 이용자 접속 및 거래량 증가*에 따른 ◁◁◁◁의 성능 부족으로 5시간 22분간 서비스가 지연**되는 장애사고를 초래한 사실이 있음***

* 전월피크일(2019.8.26.) 동시간대(10~11시) 대비 이용 접속자수 35% 증가/이체거래 12.2% 증가

** 사고 시점의 시간당 이체거래 처리 건수가 전월 피크일 대비 최고 99.3% 감소(14~15시 기준 : 43,577건 → 312건)

*** 사고발생 당일 스마트뱅킹시스템 중앙처리장치(CPU) 용량을 기존 68코어(core)에서 100코어로 32코어(약 47%)를 추가 증설하여 서비스 정상화

3) 전산자료 보호대책 위반

가) 하나프라이빗뱅킹시스템(HPBS) 관련 전산자료 보호대책 위반

◦「전자금융거래법」 제21조 제2항 및 「전자금융감독규정」 제13조 제1항 제8호, 제11호, 제4항 제2호 내지 제3호에 의하면 금융회사는 전산자료의 유출, 파괴 등을 방지하기 위하여 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하여야 하고,

전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록 및 정보처리시스템내 전산자료의 처리내용을 확인할 수 있는 사용자 로그인, 엑세스 로그 등 접근기록이 포함된 정보처리시스템의 가동기록을 1년 이상 보존하여야 하는데도,

- ㈜하나은행(▣▣▣그룹)은 검사대상기간 중 하나프라이빗뱅킹시스템(HPBS)의 게시물 관련 첨부파일을 백업*하지 않아, 하나프라이빗뱅킹시스템(HPBS) 전산자료 ◑◑,◑◑◑건**을 삭제하고 이를 복원하지 못하였고,

  * 첨부파일이 저장되어 있는 저장장치(NAS)의 파일시스템(◒◒◒◒◒◒◒◒◒◒◒◒◒◒◒◒◒◒◒◒◒◒)을 백업하지 않음

  ** 2016.12.8.~2020.2.27. 기간 중 하나프라이빗뱅킹시스템 게시판에 업로드된 첨부파일로 PB영업활동(▨,▨▨▨건), 교육세미나(▨▨건), 업무공지사항(▨,▨▨▨건), 업무공지사항(실적), 업무공지사항(추진) 등 PB가 고객을 대상으로 진행한 영업활동의 내용, PB의 실적평가 세부 내역 등

- 관리시스템(◔◔◔◔◔◔)의 가동기록을 최근 3개월만 보존하여 삭제된 전산자료 관련 접근기록을 확인할 수 없도록 운영함으로써 전산자료 유출, 파괴 등을 방지하기 위한 보호대책을 위반한 사실이 있음

나) 운영CRM 시스템 전산자료 보호대책 위반

◦ 「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제13조 제3항에 의하면 금융회사는 단말기를 통한 이용자 정보 조회시 사용자, 사용일시, 변경·조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 하는데도,

◦ ㈜하나은행(▣▣▣그룹)은 검사대상기간 중 운영CRM 시스템 내 이용자 정보를 조회할 수 있는 '손님검색창*' 시스템을 구축·운영하면서, 사용자, 사용일시, 조회내용 등을 자동 기록하였으나 10일간만 보존되도록 운영한 사실이 있음

* 영업점 및 조회 권한이 있는 본부직원이 고객 응대 등을 위해 고객을 검색하는 시스템으로, 고객의 성명 등을 입력하여 검색 시, 일치하는 이용자 정보(성명, 생년월일, 연락처, 주소 등)가 일괄 조회

4) 망분리 대체 정보보호통제 위반

◦ 「전자금융거래법」 제21조 제2항 및 「전자금융감독규정」 제15조 제1항 제3호, (舊)「전자금융감독규정시행세칙」 제2조의2에 의하면 금융회사는 내부통신망과 연결된 내부 업무용시스템은 인터넷 등 외부통신망과 분리·차단 및 접속을 금지(이하 '망분리')하여야 하고,

업무상 필수적으로 특정 외부기관과 연결해야 하는 경우 망분리 예외를 위한 자체 위험성 평가를 실시하고, 망분리 대체 정보보호통제*를 적용하여야 하는데도,

* 승인된 프로그램만 설치·실행토록 하는 단말기 보안 강화 대책 등(「전자금융감독규정 시행세칙」 [별표7])

- ㈜하나은행(◀◀◀◀본부)는 임직원 업무용 단말기에 대한 망분리 환경을 구축(2014.8월)하고 업무상 필요로 인한 망분리 예외를 허용*하면서, 2017.11.1.~2020.11.6. 기간 중 승인된 프로그램만 설치·실행토록 대책을 수립하지 아니하여**

* '행정안전부 관련 업무를 위한 LDAP서버 접속'을 업무상 필수적으로 특정 외부기관과 연결해야 하는 망분리 예외적용 처리 대상으로 지정·운영(2017.11.1.)

** 다만, 외부로부터 유입된 실행파일이 단말기 운영체제(OS)에 중대한 영향을 끼치는 위협행위(MBR, 서비스 등록, 커널 드라이버 등록, 레지스트리 변경, 인젝션 등)를 수행할 경우, 이를 차단하는 검역소 솔루션(♧♧♧♧♧♧♧♧)을 도입·운영(2014.12.22.)

- 前영업점 직원 ♥♥♥(♣♣지점 소속, 2018.7월 퇴직)이 부정 금융거래를 계획한 범죄조직과 공모하여 2017.11.10.~2018.4.30. 기간 중 업무용 단말기 및 계정계 환경을 파악할 목적으로 ▦▦개의 미승인 프로그램*을 실행**(총 ▧,▧▧▧회)하는 것을 방지하지 못한 사실이 있음

* 외부 이메일을 통해 범죄조직으로부터 미승인 프로그램을 수신하고 이를 은행 내부망으로 유입

** 실행을 시도한 총 ▦▦개의 프로그램 중 ▦▦개 프로그램은 실행이 완료되었으며, ▦▦개의 프로그램은 실행 후 검역소 솔루션(♧♧♧♧♧♧♧♧)에 의해 차단되었음

5) 전산원장 변경 통제 위반

◦「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제27조 제1항 내지 제2항에 의하면 금융회사는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함된 전산원장 변경절차를 수립·운용하여야 하는데도,

- ㈜하나은행(▣▣▣그룹)은 검사대상기간 중 계정계(상품처리) 시스템 내 자동이체원장조회 화면*을 통해 전산원장을 변경할 수 있도록 운영하면서 동 화면에 대해서는 전산원장 변경절차를 적용하지 않아,

* 계정계(상품처리)시스템의 하부 메뉴로 자동이체 처리(매일 03:00~23:50)시 예외상황(대상정보 오류 및 누락 등)이 발생할 경우, 신속하게 오류원인 파악 및 문제해결을 위해 사용

- 담당 직원(▨명)이 동 화면을 통해 총 ▥▥▥회에 걸쳐 전산원장을 변경하였음에도 변경 전후내용을 자동기록 및 보존하지 않았고, 변경내용의 정당여부에 대해 제3자가 확인하지 않은 사실이 있음

6) 공개용 웹서버 관리대책 위반

◦「전자금융거래법」 제21조 제2항, 「전자금융감독규정」 제17조 제1항 제4호에 의하면 금융회사는 공개용 웹서버의 안전한 관리를 위하여 DMZ구간 내에 이용자 정보 등 주요정보를 저장 및 관리하지 아니하여야 하고 거래로그를 관리하기 위한 경우에는 예외적으로 암호화하여 저장·관리하여야 하는데도,

- ㈜하나은행(■■■그룹)은 검사착수일 현재(2020.10.12) DMZ구간에서 운영하는 '▤▤▤ ▤▤▤▤▤▤▤' 및 '◆◆◆ ◆◆◆◆◆◆◆◆ ◆◆◆◆◆◆◆◆' 서버에 총 XXX건의 이용자 정보(영문이름, 카드 결제금액, 가맹점 정보 등)를 암호화하지 않고 평문으로 저장한 사실이 있음

□ 직원

1. 국외점포에 대한 현지 감독기관 제재 보고의무 위반

◦「은행법」 제47조 제10호 등에 의하면 은행은 은행의 국외현지법인 또는 국외지점이 현지 감독기관으로부터 제재를 받는 등 주요 변동사항이 있을 때에는 그 사실을 금융감독원장에게 지체없이 보고하여야 하는데도,

- ㈜하나은행(●●●●●(●●부)은 2015.10.12.~2019.8.15. 기간 중 국외현지법인(☆☆☆☆☆ KEB하나은행 등 4개 법인) 또는 국외지점(♧♧♧ 지점 등 2개 지점)이 현지 감독기관으로부터 제재를 받은 총 ♤♤건에 대하여 이를 금융감독원장에게 지체없이 보고하지 않고 최소 31일에서 최대 1,275일까지 지연 보고하였음

※「금융기관 검사 및 제재규정」<별표3> 과태료 부과기준에서 과태료 부과금액이 10만원 미만인 경우 과태료 부과를 면제할 수 있도록 정하고 있는 점 등을 감안하여 현지 감독기관으로부터 부과받은 과태료 금액(원화 환산)이 10만원 이상인 건만 제재대상에 포함하였음

나. 근거법규

□ 기관에 대한 조치

○ 「보험업법」 제100조(금융기관보험대리점등의 금지행위 등) 제1항 제6호, 제209조(과태료) 제2항

○ 「보험업법 시행령」 제40조(금융기관보험대리점등의 영업기준 등) 제4항, 제48조(금융기관보험대리점등의 금지행위 등) 제1항 제1호, 제104조(과태료의 부과기준), [별표9]

○ 「퇴직급여법」 제33조(퇴직연금사업자의 책무) 제5항, 제42조(권한의 위임·위탁), 제1항 제48조(과태료) 제1항 제2호

○ 「퇴직급여법 시행령」 제36조(개인형퇴직연금제도 가입자에 대한 교육사항) 제1항, 제2항, 제41조(권한의 위탁·위임) 제1항 제6호, 제42조(과태료의 부과기준), [별표3]

○ 퇴직급여법 시행규칙」 제4조(가입자에 대한 교육의 방법 및 절차 등), 제10조(개인형퇴직연금제도 가입자에 대한 교육방법)

○ 「금융기관 검사 및 제재에 관한 규정」 제20조(과징금 및 과태료의 부과) 제1항, 제3항, [별표3], [별표6]

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

○ 「전자금융거래법 시행령」 제33조(과태료의 부과기준) 및 [별표3]

○ 「전자금융감독규정」 제7조(전자금융거래 종류별 안전성 기준) 제3호, 제13조(전산자료 보호대책) 제1항 제8호, 제10호, 제3항, 제4항 제2호, 제3호, 제15조(해킹 등 방지대책) 제1항 제3호, 제17조(홈페이지 등 공개용 웹서버 관리대책) 제1항 제4호, 제25조(정보처리시스템의 성능관리), 제27조(전산원장 통제) 제1항, 제2항, 제34조(전자금융거래 시 준수사항) 제5호

○ 舊「전자금융감독규정시행세칙」(2020.11.6. 개정되기 전의 것) 제2조의2(망분리 적용 예외) 제1항, 제3항, [별표7]

□ 직원에 대한 조치

○ 「은행법」 제47조(정관변경 등의 보고) 제10호, 제65조(권한의 위탁), 제69조(과태료) 제5항 제7호

○ 「은행법 시행령」 제24조의2(정관변경 등의 보고) 제1항, 제2항 제1호, 제26조의2(권한의 위탁) 제1항, 제31조(과태료의 부과기준), [별표3], [별표4]

○ 舊「은행법 시행령」 (대통령령 제32640호로 개정되기 전의 것) 제24조의2(정관변경 등의 보고) 제1항, 제2항 제1호

○ 舊「은행법」(법률 제17293호로 개정되기 전의 것) 제69조(과태료) 제4항 제7호

○ 舊「은행법」(법률 제14826호로 개정되기 전의 것) 제69조(과태료) 제4항 제7호

○ 舊「은행법 시행령」(대통령령 제28382호로 개정되기 전의 것) 제31조(과태료의 부과기준), [별표4]

○ 「질서위반행위규제법」 제3조(법 적용의 시간적 범위)