
	보도 참고자료	
	배포시부터 보도 가능	

작성부서	금융위원회 중소기업과, 서민금융과, 전자금융과 금융감독원 여신전문검사실, IT감독국, 특수은행검사국, 서민금융지원국		
책임자	이운수 과장(2156-9850) 이형주 과장(2156-9470) 전요섭 과장(2156-9490) 류찬우 실장(3145-8810) 송현 국장(3145-7180) 이종욱 국장(3145-7200) 양현근 선임국장(3145-8150)	담당자	중소금융과 이종림 사무관 2156-9856 서민금융과 김영대 사무관 2156-9472 전자금융과 김종훈 사무관 2156-9491 검사2팀 김준환 팀장 3145-8822 IT총괄팀 김윤진 부국장 3145-7182 검사2팀 김재경 팀장 3145-7228 신용정보팀 남택준 부국장 3145-8140
배포일	2014.1.8(수)	배포부서	대변인실(2156-9543~48) 공보실(3145-5789~92) 총 4대

제 목 : 신용카드업자 고객정보 유출 관련 현황 및 대응방안

<p>I. 사고개요</p> <p>□ 창원지검(특수부)은 신용정보회사(KCB) 직원 100을 3개 신용카드업자 (KB카드, 롯데카드, NH카드)로부터 고객 정보를 대량으로 불법 수집·유포한 혐의로 기소했다고 중간 수사결과 발표(14.1.8일)</p> <ul style="list-style-type: none"> ○ 100은 신용카드업자의 위·변조 방지 시스템 개발 용역 작업 과정에서 카드 회원의 개인정보 등을 불법으로 수집하였으며, 동 자료는 대출광고업자 및 대출모집인에게 유출됨 ○ 유출된 정보는 회원의 성명, 휴대전화번호, 직장명, 주소 등 개인정보* (신용카드 사용 등과 관련된 신용정보 일부 포함)인 것으로 파악 <p>* KB카드 약 5,300만명, 롯데카드 2,600만명, NH카드 2,500만명</p> <p>□ 검찰은 개인정보 불법 수집자 및 최초 유통자가 검거되어 외부에 유출·확산되지 않은 것으로 판단(추가 유출 여부는 계속 수사중)</p>
--

II. 대응방안

➔ 금번 사고에 대해 금융위와 금감원은 사고발생의 원인을 신속히 진단하고 재발 방지 및 피해 확산 차단에 주력할 계획

1. 해당 신용카드업자 ➔ 즉각적인 검사 및 제재 조치

- 사고가 발생한 3개 신용카드업자에 대해서는 개인정보 유출 경로 등이 파악되는 즉시 금감원이 현장 검사를 실시
 - 정보가 유출될 때까지의 금융회사의 정보보호, 내부통제 장치가 제대로 관리·운영되고 있었는지 집중 검사
 - ※ 기존의 금융회사 사고가 제3자의 해킹, 내부직원에 의한 정보 유출이었다면, 同件은 협력회사 직원이 의도성을 가지고 자료를 유출했다는 점이 특징
- 금감원 검사에서 드러난 위법 사항에 대해서는 “일벌백계” 차원에서 관련 법규에 따라 엄중 제재
 - 권한 없는 자가 무단으로 정보를 유출하는 등 금융회사의 관리·운영상 취약점이 드러날 경우 「전자금융거래법」 위반* 등으로 신용카드업자에 대해서는 영업정지, 임·직원은 해임권고 등 중징계 가능
 - * 전자금융거래법: 전자금융거래의 안전성 확보 의무(§21)
전자금융감독규정: 업무자별 단말기 접근권한(§12) 및 전산자료 보호대책(§13) 등
 - 특히, 최고 관리자가 전산자료 보호 등 금융거래의 안전성 의무를 다했는지에 대해서도 철저히 따져 책임을 물을 계획
 - * (금융기관 검사 및 제재에 관한 규정 시행세칙) IT사고 등으로 금융회사의 건전경영 및 이용자의 권익을 심하게 해치는 등 사회적 문제를 야기시킨 경우 경영진 등 감독자에 대하여는 행위자와 동일한 수준 제재 부과 가능

2. 금융회사의 개인·신용 정보 처리의 적정성 일제 점검

- 사고가 발생하지 않은 금융회사에 대해서도 고객정보 유출 방지대책 및 고객정보 관리의 적정성 실태를 전면 점검
 - 금감원은 '14.1월중 금융회사 자체 점검 체크리스트*'를 마련
 - * 내부직원·외부 용역직원의 정보 접근권한 부여현황 및 정기적으로 동 부여 권한의 적정성 점검 여부 등
 - 금융회사별로 체크리스트를 기초로 자체 점검을 실시('14.1월~2월중)하고, 그 결과 및 미비점에 대해서는 보완계획을 제출
- 금감원은 자체 점검 결과를 검토하고, 취약하거나 미흡한 금융회사에 대해서는 추가 현장 점검 실시 및 보완 유도

3. 유출 정보에 대한 추가 피해 확산 차단

- 사고가 발생한 신용카드업자는 회원에게 고객정보 유출 항목, 유출 시점 및 경위, 피해방지 최소화 대책(카드 재발급 등) 등을 서면, e-mail, 문자 등으로 개별 고지하고, 자사 홈페이지 등에도 게재
 - 보이스피싱, 대출사기, 불법사금융 등 우려되는 추가 피해 예방을 위한 유의사항*도 함께 안내
 - * 금융회사 사칭이 의심되는 전화나 문자메시지 주의, 대출실행과 관련한 금전 요구시 대출사기 의심, 문자메시지에 포함된 출처가 불분명한 인터넷주소 클릭 주의 등
- 금감원에 “정보유출 감시센터”를 설치·운영하여 유출된 정보의 불법 유통 사례를 접수
 - * 신고자는 금융거래 정보의 매도·매입자, 거래되는 사이트, 유출 금융회사 등 불법 금융거래 유통 관련 정보를 제시

- 접수된 사례는 확인 후 수사기관에 통보하는 한편, 정보유출 관련 금융회사에 대해 신속한 조치를 지도하여 피해 확산 억제
 - 불법으로 유출된 정보를 추가로 이용하거나 매매한 제3자 역시 형사처벌*이 가능한 만큼 유출 정황 인지시 즉시 수사기관에 통보
 - * 신용정보 등을 부당하게 유출한 자와 동 정보를 넘겨받은 자는 「신용정보보호법」, 「전자금융거래법」 등 관련 법령에 따라 5년 이하(전자금융거래 정보는 7년 이하)의 징역 또는 5천만원 이하의 벌금형 가능

4. 금융회사 개인정보보호관련 재발방지 대책

- 정보보호 관련 기관과 협력하여 “개인정보보호 강화 종합대책” 마련 추진
 - 최근 발생한 개인정보 유출사고의 주요 유형 및 취약점을 분석하고
 - 개인정보 접근·취급과 관련한 내부통제시스템 및 보안대책 전반에 관한 제도개선 사항을 검토
 - 특히, 정보기술관련 ‘업무처리 위탁’이 증가함에 따라 제기되는 관련 위험요소 및 대응방안을 집중 검토
 - 필요시 개인정보 유출관련 ‘제재범위’ 및 수준의 상향조정방안 검토
 - * 예) 신용정보회사처럼 정보처리관련 업무를 주로 수탁 받아 처리하는 회사의 경우 업무수행 직원교육 및 관리책임 미비시 기관경고·영업정지 등 행정제재 도입 등 검토

Ⅲ. 향후계획

- 금감원이 3개 신용카드업자에 대한 검사 실시: '14.1월중
- 금융회사 체크리스트 마련(금감원) 및 금융회사 자체 점검: '14.1~2월
- “정보유출 감시센터” 설치·운영: '14.1월중
- 개인정보보호 강화 종합대책 마련을 위한 협의체 운영: '14.1/4분기



☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다.

<http://www.fsc.go.kr> / <http://www.fss.or.kr>

