금융사 개인정보 유출 방지 방안에 관한 연구

정기석*

요 약

올 들어 카드3사를 비롯한 개인금융정보 유출 사건이 끊임없이 발생되고 있다. 이는 개인정보의 암호화 미비와 인적 보안의 태만 등 원칙을 지키지 않은데 그 원인이 있다. 또 유출된 불법정보를 활용해 영업을 하는 모집인들이 수요처로 작용하는 것도 유출 원인중 하나로 분석되고 있다. 정보 유출은 개인에게는 정신적 피해와 함께 2차 피해를 줄 수 있으며 해당 금융사에는 영업 손실을 가져올 뿐만이 아니라 신뢰성을 악화시키고 나아가 지금까지 쌓아온 신용사회의 근간을 무너뜨릴 수 있다는 점에서 철저한 재발방지가 요구된다. 이에 정부에서는 사후제재강화와 개인정보 수집·보유·제공 제한을 골자로 하는 금융분야 정보유출 방지 종합대책을 발표하기에 이르렀고 국회에서는 관련법 개정안 심의가 진행되고 있다. 본 논문에서는 개인정보유출의 원인을 분석하고 정부 대책의 실효성에 대해 따져보고 정보유출방지를 위한 개선방안을 모색해 본다.

A Study on Measures for Preventing Personal Information Leakage in Financial Corporations

Jeong Gi Seog*

ABSTRACT

Personal information leakage in financial corporations including three card corporations has occurred constantly this year. It is due to incomplete encryption system and negligent personal security. Solicitors are known as a cause of information leakage because they operate with leaked information. Information leakage can cause secondary damage with mental demage to person and result in a drop in reliability as well as an operating loss in financial corporations. Also because it can destroy a base of credit society, prevention of recurrence is badly needed. The government finally announced 'general measures for prevention of information leakage in the field of finance' with sanctions reinforcement and restriction to collect, possess, provide personal information as the main agenda. And a related law revision is going in the National Assembly. In this paper, effectiveness of government measures is weighed with the cause analysis of information leakage and countermeasure for prevention of information leakage is found.

Key words : Personal information leakage, Encryption, Personal security, Credit society

접수일(2014년 5월 30일), 수정일(1차:2014년 6월 25일, 2차:2014년 6월 27일), 게재확정일(2014년 6월 29일)

* 영동대학교 정보통신보안학과

1. 서 론

KB국민, 롯데, NH농협 등 카드3사의 정보유출[1], 보험사GA 고객정보유출[2], 포스단말기관리업체 서버에서 신용카드정보 유출[3], 농협생명 정보유출[4] 등 개인금융정보 유출사고가 끊임없이 발생하고 있다. 이는 개인금융정보를 필요로 하는 수요가 그 주요 원인으로 분석되고 있다. 카드모집인이나 대출모집인 등이 유출된 불법정보를 영업에 활용하고 있기 때문이다. 이에 정부는 카드 3사 사건이후 금융회사 고객정보유출 재발방지 대책[5], 개인정보 불법유통·활용 차단조치[6]를 발표했고 이들을 종합해서 금융분야 개인정보유출 재발방지 종합대책[7]을 발표하기에 이르렀다.

국회에서도 개인정보 유출 방지법 개정을 추진하여 4월 임시국회에서 전자금융거래법, 금융지주회사법 개정안을 통과시키고 신용정보법은 논란 끝에 통과가 미뤄져 6월 임시국회로 넘어가게 되었다. 또한 5월 2일 국회 본회의에서는 정보보호 법률 사상 처음으로 정보유출 관련 이용자 피해를 금전적으로 보상(300만원 이하)하도록 명시한 법정손해배상제(정보통신망법)가 통과되었으며 주민등록번호에 대한 예외없는 암호화(개인정보보호법)는 2월에 통과된 바 있다.

카드3사의 고객정보유출 사태는 정부의 관리·감독 소홀에 따른 예견된 인재임이 감사원 감사 결과 드러났고[8] 금융기관 역시 원칙에 충실하지 않아 암호화 등 기본적인 조치를 하지 않은 점이 유출 원인으로 지적되고 있다. 카드3사 사건 후 600만 건의 해지와 탈회가 있었고 3개월간의 영업정지로 인한 손실이 1000억 원으로 추정되고 있다. 또 업계에서는 해당 3사의 올해 예상 순이익은 2500여억 원으로 2013년 4200여억 원에 비해 절반가량 줄어들 것으로 보고 있다[9]. 또 진행되고 있는 피해보상 소송도 부담이다. 그리고 경제적 손실 외에 무엇보다도 중요한 것은 신뢰성 추락이다. 신용사회의 신뢰가 무너져 회복하는데 상당한 시간이 걸릴 수 있다는 우려가 나오고 있다. 이렇듯 금융정보유출은 회사에 수익성 악화를 가져올 뿐만 아니라 신용사회의 기반을 무너뜨릴 수 있다는 점에서 방지대책을 철저히 하여 재발되지 않도록 해야 한다. 따라서 본 논문에서는 개인금융정보의 유출 원인과 금융보안관리 실태를 알아보고 정부대책의 실효성에 대해 따져보고 정보유출 방지를 위한 개선방안을 제시한다.

2. 금융사 보안의 문제점

2.1 개인금융정보 유출 원인

2.1.1 금융당국의 감독 소홀

금융당국의 금융회사 관리·감독 소홀이다. 금융당국은 은행과 카드, 보험, 증권사 등의 IT 부문 검사와 관련해 운영실태 평가를 하도록 한 규정을 지키지 않아 최근 5년간 144개 금융사중 보험 개발원 등 46개 금융기관이 실태평가를 전혀 받지 않았다. 또한 은행연합회를 포함한 26개 금융기관은 종합검사격인 IT검사조차 받지 않았다. 당국은 금융회사가 외주업체에 대한 보안관리를 체계적으로 할 수 있는 규정을 갖추지 않아 시중은행 5곳의 용역업체 직원 컴퓨터에 '전산망 구성도'같은 주요정보가 저장될 수 있게 했다.

2.1.2 정보의 과도한 수집 및 불법정보 수요

금융회사 등이 영업에 필수적이지 않은 정보까지 과도하게 수집하여 장기간 보유해 왔다. 일반적으로 약 20여 개(예: 전화번호, 주소) 많은 경우 약 50여 개 항목을 수집해 왔다. 불필요하게 많이 수집된 개인정보에 대한 관리소홀로 유출되는 것이다. 제3자 제공시 목적도 불분명한 포괄적 동의 등으로 인해 사실상 동의가 강요되는 등 불합리한 관행이 지속되어 왔다. 본인이 잘 모르는 수백 개의 제휴사 등(제3자)에 신상정보가 제공되었다. 또한 대출모집인 등(대출모집인, 대부중개업자, 보험설계사, 카드모집인 등)이 무차별적 모집·권유 영업을 하는 과정에서 불법정보의 수요처로 작용하고 있다. 이러한 대출모집인 등을 활용해 금융회사는 고객 모집이라는 편익을 받음에도, 이들에 대한 관리책임은 부족한 실정이다.

2.1.3 금융사 내부통제 부실

이사회, CEO 등 주요 의사결정자에 대해 정보보호 현황에 대한 충분한 보고가 이루어지지 않고, 관심이 부족하다. 금융회사의 영업중시 관행으로 고객정보 관리에 소홀하고 보안규정도 준수하지 않는 등 내부통제가 미흡하다. 그 동안 정보유출 사고 발생시에도 형식적 규정 준수로 면책이 되면서 정보보호와 관련한 주의가 부족한 실정이다. 또한 정보보호책임자(CISO)가 부재이거나 최고정보책임자(CIO)가 겸직한다. CIO는 회사가 보유한 정보를 활용해 사업전략을 구상하는 반면 CISO는 회사의 정보 보안과 관리를 책임지는 역할로 CIO를 견제하는 입장이다. 따라서 한 사람이 두 직책을 겸할 경우 CIO 견제라는 CISO의 역할이 사실상 불가능해진다.

2.1.4 금융사에 대한 불충분한 제재

정보유출시 금융회사 등에 대한 제재 수준이 미미하여 재발방지 효과가 미흡했다. 신용정보법상의 제재가 개인정보보호법상의 제재보다 낮은 수준이다.

<표 1> 신용정보법과 개인정보보호법의 제재 비교

정보유출시	과태료	형벌	과징금
신용정보법	1천만원 이하	5년 이하 징역,5천만원 이하 벌금	없음
개인정보 보호법	3천만원 이하		5억원 이하

금융회사가 정보를 유출하거나 불법정보를 활용하는 경우에도 충분한 금전적·형사적 제재 미부과로 정보관리가 허술했다. 그동안 개인정보 유출시 해당 금융기관에 대해 낮은 수준의 과태료(최고 600만원) 부과 및 임·직원에 대해서도 '주의' 수준의 가벼운 제재를 부과했다.

2.2 금융보안 실태

2.2.1 CISO 현황

현행법(전자금융거래법)상 종업원수 300명 이상의 금융회사는 CISO를 임원으로 임명해야 한다. 3월말 현재 국내 50개 대형 금융회사중 임원급CISO가 있는 곳은 16곳(28%)으로 3월초에 비해 2곳 늘었다. 나머지 34개 금융사중 23개사는 CIO가 CISO를 겸직하고 있고 5개사는 부장급 직원이 양쪽업무를 맡고 있으며 5개사는 CISO담당부장만 있다. 1개사는 CISO가 없다[10].

<표 2> CISO보유현황

구분(50)	카드사(8)	증권사(10)	손해보험사(9)	생명보험사(9)	금융지주(5)	은행(9)
CISO임원(16)	신한,KB국민,롯데,삼성,하나SK,현대	KDB대우,메리츠종금,미래에셋,하나대투	삼성화재,한화손해보험	미래에셋생명	우리금융지주,KB금융지주	국민은행
CIO가 CISO겸직(23)	우리, BC	대신증권,신한금융투자,한국투자증권,현대증권	(6)	(7)		하나,시티SC은행,농협은행
부장급 CIO가 CISO겸직(5)		삼성증권	농협손보	농협생명,		우리은행,외환은행
부장급 CISO(5)		우리투자증권			농협금융지주,신한금융지주	신한,기업
없음(1)					하나금융지주	

업종별로는 정보유출이 작은 카드사와 증권사의 CISO선임비율이 높았다. 임원급CISO가 있는 곳은 카드사 8곳중 신한, KB국민, 롯데, 삼성, 하나SK, 현대카드 등 6개사이고 대형 증권사 10곳 중에서는 KDB대우, 메리츠종금, 미래에셋, 하나대투 등 4개사, 9개 손해보험사 중에서는 삼성화재와 한화손해보험 등 2곳. 9개 생명보험사 중에서는 미래에셋생명 1곳, 금융지주(5)와 은행(9) 중에서는 우리금융지주와 KB금융지주, 국민은행 등 3곳이다. CIO임원이 CISO를 겸직하는 곳은 은행(4), 보험(13), 카드(2), 증권(4) 등 23개사이다. 임원이 아닌 부장급 CISO를 둔 곳은 농협금융지주, 신한금융지주, 신한은행, 기업은행, 우리투자증권 등 5곳이다. 부장급 CIO가 CISO를 겸직하는 곳은 농협생명, 농협손보, 우리은행, 외환은행, 삼성증권 등 5곳이다[11].

2.2.2 모집인 현황

● 카드모집인 현황

정보유출사고가 난 3사의 모집인 추이는 사고 이후 3월까지 꾸준히 감소한 것으로 나타났다. KB국민카드는 1월 1200명에서, 2월 1100명, 3월 1000명으로 매달 100명씩 감소했고 롯데카드는 1월 2000명에서 2월 1800명으로 줄어든 뒤 3월에도 비슷한 수준을 유지했다. NH농협카드는 1월 640명에서 2월 600명으로 줄고 3월에도 소폭 줄었다. 영업정지기간(2.16~5.16)에 3개 카드사가 각각 65%에서 70%까지 모집인 수수료를 보전해 줬지만 카드모집인 이탈은 계속되었다. 그러나 전체 카드모집인 숫자는 3월말 기준 3만 4882명으로 전달 3만3891명보다 1000여명 늘었다. 1월말 수준(3만 4894명)을 회복한 것이다. 이는 경제가 어려워 기존 모집인들의 빈자리를 생각보다 빠르게 채우고 있는 것으로 보인다[12].

5월17일 카드3사의 영업이 재개되면서 카드3사는 모집인과 신상품출시를 통해 잃어버린 고객을 되찾으려 하고 있고 그 외 카드사들도 모집인을 충원하며 영업력 확대를 꾀하고 있다. 불법정보 활용으로 카드모집인이 문제가 되고 있음에도 카드사들은 모집인을 이용한 영업전략을 계속하고 있다.

● 대출모집인 현황

대출모집인 제도는 1996년 씨티은행이 도입했다. 낮은 비용으로 대출 영업을 할 수 있다는 '선진' 영업방식을 2001년 국내 금융회사들도 앞다투어 도입했고 대출모집인수는 2014년1월 기준 1만 3천여 명으로 전체 금융사 대출의 20%를 담당하였으나 3월말 1만120명으로 크게 감소했다[13]. 그 이유는 카드3사 사건 이후 대출모집인들이 적법한 절차로 얻은 개인정보로 영업을 했는지 대출해주는 금융회사가 직접 확인하도록 함으로써 전에는 대출중개인들이 돈이 필요한 사람을 금융회사에 소개만 해주면 되었지만 이제는 금융회사가 고객에게 '개인정보를 활용한 마케팅에 동의했는지'를 확인해야만 대출이 되기 때문에 대출인의 입지가 그만큼 좁아졌기 때문으로 보인다.

2.2.3 주민번호 암호화 추진 현황

주민번호를 암호화하면 데이터베이스(DB)에 저장·이용할 때 암호화 과정을 거치기 때문에 전산 시스템도 용량이 더 커지고 속도도 더 빨라져야 금융업무를 진행할 수 있다. 현재 은행권에서는 2013년 우리은행, 전북은행 등이 차세대 시스템으로 개편했다. 대부분의 금융회사는 차세대 시스템을 개편하는 주기가 10년 정도다. 전북은행은 시스템 개편과 함께 주민번호 암호화도 함께 도입했다. 현재 주민번호 암호화가 되어있는 유일한 은행이다. 농협, 기업, 부산, 대구, 경남은행은 올해 차세대 시스템으로 개편하면서 주민번호 암호화도 함께 도입할 예정이다. 국민은행은 2010년, 하나은행은 2009년에 차세대 시스템을 도입했기 때문에 이들은 2020년은 되어야 주민번호 암호화와 함께 시스템 개편을 할 것으로 보인다. 하나은행은 2009년 이후 계속적으로 컨설팅 등을 통해 시스템을 보완하고 있다. 증권사에서는 삼성증권, 키움증권이 2013년에 차세대 시스템을 도입한 상황이다. 이들은 암호화 모듈만 적용하면 된다. 나머지 증권사들은 2020년까지 차세대 시스템 구축과 함께 주민번호 암호화를 추진해야 한다. 보험사의 경우에는 NH농협손보, KDB생명이 2013년에 차세대 시스템 구축을 완료했다. 올해는 코리안리재보험과 NH손해보험이 차세대 시스템을 구축할 예정이다[14].

2.3 정부대책의 타당성 검토

2.3.1 사후제재 강화

개인정보를 유출하거나 불법활용한 금융회사에 대해서는 사회적 파장 등을 감안하여 대폭 상향된 징벌적 과징금을 신설하기로 하고 불법정보 활용시에는 관련 매출액의 일정비율(예 : 3%)을 상한으로 설정(금액은 사실상 무제한)하고, 관리소홀 등으로 정보를 유출(분실·도난 등)한 경우는 일정 금액(예 : 50억원)을 상한으로 설정하였다. 금융회사 정보유출이 타업권 등에 비해 사회적 파급효과가 큰 점을 감안하여 금액상한은 타법 사례보다 높은 수준으로 설정한 것이다. 또 개인정보 유출이나 불법활용시 형벌수준을 금융관련법 최고 수준으로 크게 상향하기로 하였다. 이는 확대·재생산 위험이 높은 개인정보의 특성을 감안하여 정보유출·불법 활용시 위반행위 당사자에대한 처벌을 강화한 것이다.

<표 3>사후제재의 기존내용과 개선내용 비교

제재	위반 내용	기존 형량	3.10대책	적용 대상
징벌적 과징금	불법정보 활용		관련매출액 3%	회사
	관리소홀로 인한정보유출		최고 50억원	회사
형벌	정보유출관련 (신용정보법)	5년이하 징역이나 5천만원 이하 벌금	10년이하 징역이나 1억원 이하 벌금	신용정보제공.이용자 (은행,카드 등)
	정보유출관련 (전자금융거래법)	7년이하 징역이나 5천만원 이하 벌금	10년이하징역이나 1억만원 이하벌금	전자금융정보처리자
과태료	정보유출 방지를 위한 보안장치 미비	신용정보법 600만원	5천만원	회사
	신용정보관리인이 CEO에 정보보호관련 보고의무 해태	신용정보법	5천만원 신설	회사
	식별정보 암호화 조치 미비·정보폐기 의무 위반	신용정보법	3천만원 신설	회사
	안전성 확보의무 위반	전자금융거래법	5천만원 신설	회사
행정 제재	CEO등 임원	'주의'	행위자 책임 부과	
	신용정보회사		영업정지(6개월 이내) 또는 이에 갈음한 과징금을 부과하고 3년내 재위반시 허가취소	
	개별금융사	영업정지 3개월	6개월	

정보유출이 일어나지 않더라도 금융회사가 보안대책 미비 등 주의의무를 다하지 않을 경우 과태료수준도 대폭 강화하기로 하였다. 이는 사전에 정보유출방지를 위한 주의의무를 다하지 않은 과실 등에 대한 책임을 물어 사고 예방효과를 높일 필요가 있기 때문이다. 금융회사 임·직원에 대한 제재, 영업정지 등 기관제재도 보다 엄격히 개선하였다. 그러나 징벌적 과징금은 관련매출액 산정이 어려워 효과가 의심스럽다. 4월 국회 정무위에서는 손해액의 3배를 배상하는 징벌적 손해배상을 내용으로 하는 법안(신용정보법)이 정무위 법안심사 소위를 통과하였으나 입증책임을 둘러싼 논란으로 정무위를 통과하지 못하여 6월 임시국회로 넘어가게 됨에 따라 징벌적 과징금은 올해 시행이 불투명해졌다. 형벌, 과태료, 행정제재도 법개정 사항으로 4월 국회에서 법 개정이 무산되어 6월 국회에서 다시 논의하게 되었다.

2.3.2 금융회사의 책임강화와 모집인 관리강화

CEO 등 주요 의사결정자가 정보보호와 보안에 대해 관심이 부족하고 정보보호책임자의 역할도 제한적이었던 문제를 개선하기 위하여 정보보호 현황 및 정책을 매년 작성(연차보고서)하여 CEO 및 이사회가 직접 보고를 받도록 하고, 감독당국에도 제출하게 하였다. 정보이용·제공·보호관련 책임, 임직원·전속 모집인 등 정보보호 교육 및 보안규정 준수 점검 등의 업무를 하는 신용정보 관리·보호인을 임원으로 두도록 하고 권한도 강화하기로 했다. CISO가 정보보호 효율성을 강조하는 업무 담당시 발생하는 이해상충 방지를 위해 일정규모 이상 금융회사의 CISO는 타 IT 관련 직위와 겸직을 제한하기로 했다. 4월 국회에서 CIO와 CISO의 겸직을 금지하는 전자금융거래법개정안이 통과되어 지금까지는 CIO가 CISO를 겸직하는 경우가 많았으나 앞으로는 임원급 CISO를 독자적으로 두어야 한다. 그러나 CISO가 전사적인 보안을 수행하기는 어렵기 때문에 이사회와 최고경영진의 책임을 강화해야 한다.

금융회사가 모집인에게 정보 제공시에는 최소한의 정보만을 암호화하여 제공하고 제공된 정보는 업무목적 외 사용을 금지하고, 정보활용·파기 관리대장을 작성하여 주기적으로 점검하도록 했다. 모집인이 정보유출이나 불법정보 활용시 모집인뿐만 아니라 금융회사에 대해서도 엄정한 책임(과징금 등)을 추궁하여 과징금, 형벌(3년 이하 징역, 3천 만 원 이하 벌금), 과태료(1천 만 원 이하)를 부과하기로 했다.

2.3.3 자기정보결정권 보장

개인이 본인정보를 보호할 수 있도록 요청할 수 있는 권리인 자기정보결정권을 보장하도록 했다. 본인의 신용정보가 어떻게 이용·제공되고 있는지 확인을 요청(정보 이용현황 조회권)할 수 있고 금융회사에 영업 목적으로 전화 등의 연락을 하지 말라(Do

not call)고 할 수도 있다(연락중지 청구권). 기존에 동의했던 정보제공을 철회할 수 있고(정보제공 철회권) 거래가 끝난 후 금융회사가 보유한 자신의 정보에 대해 파기·보안을 요구할 수 있다(정보보호 요청권). 명의도용 피해 방지 등을 위해 고객이 요청하는 경우, 대출, 카드발급 등을 위한 신용조회를 일정기간 중지할 수도 있다(신용조회 중지 요청권). 연락중지 청구권은 현재도 가능하지만 나머지는 신용정보법 개정사항이다.

2.3.4 개인정보 수집 제한

계약체결에 필수적인 정보와 선택 가능한 정보를 구분하여 필요최소한의 정보만 수집하도록 하였다. 현재 금융업권별·상품별로 20~50여개인 수집정보 항목을 필수항목(6~10개)과 선택항목으로 구분하고 최소화하였다. 주민번호는 금융부문에서 신용도 조회, 과세기반 확보(금융소득종합과세 등)를 위해 수집은 불가피하나, 수집방식·보관을 엄격히 제한하기로 했다. 수집은 최초에만 고객이 직접 인증센터와 연결된 전자단말기에 입력(Key-in)하고, 이후에는 주민번호 기입없이 신원확인 절차만 거치도록 하여 노출을 최소화하도록 했다. 금융회사는 수집한 주민번호는 외부망은 물론 내부망에도 암호화하여 보관·이용하여야 한다. 주민번호의 예외없는 암호화를 규정하는 개인정보보호법 개정안이 국회 통과를 했기 때문에 법적 근거도 마련되었으나 회사규모, 이용고객 수 등을 고려하여 단계적으로 시행할 계획이다. 이는 한꺼번에 암호화하는 일은 비용과 시간측면에서 결코 쉽지 않기 때문에 금융사 사정을 고려한 금융당국의 배려로 5년을 유예한 것이다. 또 암호화 추진과정에서 그간 기준 없이 방만하게 열어둔 고객정보 공유 실태가 드러나는 것에 대한 두려움도 반영되었을 것이다[15].

2.3.5. 정보 보유·활용·제공 제한 및 파기 의무화

금융지주 내에서 고객의 사전 동의 없이 계열사 보유정보를 제공받아 금융상품 판매 등 외부영업에 이용하는 것을 제한하기로 했다. 단, 그룹단위의 신용위험관리, 고객분석 등 내부 경영관리를 위해 필요한 경우에는 계열사간 고객정보 제공을 계속 허용하기로 했다. 제공받은 정보는 이용기간을 1개월 이내로 제한하고, 이용기간 도과시 영구 파기여부를 고객정보 관리인이 확인하도록 했다. 이를 뒷받침하는 금융지주회사법 개정안이 국회를 통과(5월)했다.

제3자 정보제공시 포괄적 정보제공 동의를 제한하여, 계약 체결에 필수적인 제3자와 선택적 제3자를 구분하여 동의를 받도록 했다. 제3자에 제공되는 목적 또는 혜택을 분명히 적시하고 이용목적에 부합하는 정보만을 한정하여 제공하여야 한다.

거래종료 후에는 원칙적으로 필요한 정보(식별정보, 거래정보 등)만 보관하고 즉시(3개월 이내에) 파기(학력, 직업·직위 등의 정보)하고 현재 거래중인 고객의 정보와 분리하여 보관해야 한다. 2단계로 거래종료 후 5년이 경과한 정보는 원칙적 모두 파기해야 한다. 제3자가 제공받은 정보를 이용하는 필요최소한 기간을 설정하고 기간 도과시 제3자는 파기 의무화하도록 했다.

<표 4> 3.10 개인정보 유출 재발방지 종합대책 주요 내용

대책	주요 내용
처벌수위 강화	• 불법정보 활용시 관련매출액 3%까지 과징금 • 신용정보회사 정보유출시 6개월 영업정지 또는 과징금, 3년내 재발시 허가 취소 • 금융회사 정보유출시 영업정지 6개월 • 정벌적손해배상제도, 배상명령제도 도입 검토
제한적인 개인정보수집	• 결혼기념일,종교,가족정보 수집 금지 • 주민등록번호는 최초 1회만 수집 • 필수정보와 선택정보로 구분해 수집
엄격한 개인정보 보유.활용	• 금융지주회사 계열사 정보제공 시 1개월 이내 삭제 • 제3자에게 부가서비스 위한 필수 정보만 제공 가능 • 고객 동의 없는 비대면 영업 금지
파기요건 강화	• 거래종료 3개월 후 파기, 불가피한 경우 영업목적 사용불가 • 고객이 본인정보 파기 요구

3. 제안하는 정책 방향

3.1 법과 감독체계 정비

개인정보 불법 유출은 사회안보 차원서 다뤄야 한다. 불법 유출된 개인정보를 활용한 금융범죄는 고도

신용 사회의 근간을 흔드는 일종의 체제안보와 관련된 중대 범죄이다. 따라서 금융사든, 개인이든, 불법 정보라는 것을 알고도 활용할 경우의 처벌에 대해선 일반법인 신용정보법이나 다른 기존 개별법보다 훨씬 강화된 기준이 본격 논의될 필요가 있다. 그리고 금융사의 개인정보 보호는 국가안전처에서 맡아야 한다. 관경유착이 뿌리깊은 우리나라에서 금융사의 개인정보 관리를 금융당국에 맡기는 것은 곤란한 점이 있다. 또 개인정보 관리는 정보보안 분야로 기술적인 분야이다. 따라서 금융당국보다는 IT를 담당하는 미래창조과학부나 재난전담부서인 국가안전처에서 담당해야 한다. 행정적인 규제만 할 것이 아니라 실질적으로 도움이 되는 기술적·관리적보안 방안과 재정지원이 필요하다. 또한 정부 책임자 처벌을 강화해야 한다. 정부 대책에는 금융사에 대한 책임강화와 제재는 포함되어 있으나 정부 책임자에 대한 처벌 내용은 들어 있지 않다. 당국의 과실이 드러나면 책임자를 일벌백계해야 정부의 감독기능이 강화될 것이다.

3.2 피해자 보상제도 도입

배상명령제도, 집단소송제 도입이 필요하다. 현재 금융감독기관에 분쟁조정절차가 있는데 이는 금융소비자의 입증 책임이 완화되는 측면이 있지만, 이 절차가 효력을 얻기 위해서는 양자가 합의에 성공해야 한다는 부담이 있다. 또 분쟁조정 절차를 진행 중이더라도 한 쪽에서 소송을 제기하면 분쟁조정 절차는 끝나고 소송으로 곧바로 넘어가게 되면서 분쟁조정 절차 자체를 무력화시킨다. 소송을 할 경우 금융회사의 잘못을 소비자가 입증해야 하는 어려움이 있다. 소송을 진행하면서 금융사 잘못을 입증하려면 증거가 필요한데, 그 대부분의 증거를 금융회사가 가지고 있다는 것이 문제다. 따라서 피해자가 주요 정보에 대해 접근할 수 없게 되다보니 결국 금융사의 고의와 과실을 입증해 내기가 어렵게 되어 있다.

배상명령제도는 영국의 금융감독청이 관련 법령 위반자 또는 위반사실을 알면서도 이에 관여한 자를 상대로 발생한 이익이나 손해 등을 배상하도록 명령할 것을 법원에 신청하거나 직접 명령하는 제도에서 비롯된 것으로 우리나라에도 이미 존재한다. 공정거래위원회가 불공정거래 행위에 대한 손해 여부를 조사해 위반한 사업자에게 손해배상명령을 내리는데, 이 명령을 내리게 되면 이것으로 인해서 금융사와 금융소비자 간 다툼이 어느 정도 해결되는 모습도 현재 보이고 있다. 또 집단소송제는 현재 증권거래로 인한 피해에 대해서만 인정되고 있는 것으로 금융관련 전 분야로 확대할 필요가 있다.

3.3 사전제재와 예방 강화

교통법규에 범칙금을 부과하듯 사소한 정보유출 법규 위반에 대한 제재를 하여야 한다. 또 가트너의 연구 결과에 따르면 정보유출사고의 복구가 5.6달러의 비용을 발생시킬 때 예방비용은 1달러밖에 들지 않는다고 한다[16]. 개인정보 대책을 기업이나 개인에게 맡기지 않는다. 즉, 정부는 기업이나 개인에게 정보보호 비용을 전가하지 않는다. 예로 기업의 암호화 시스템 구축을 경제적으로 지원하고 개인의 OTP나 보안토큰 구입을 정부에서 보조하여 무료서비스 하여야 한다.

3.4 정보보호에 대한 인식 제고

정부 및 금융회사는 물론 소비자의 정보위기에 대한 불감증을 시정하고 개인정보 유출에 대한 인식을 제고하여야 한다. 정부의 대책과 함께 실천 의지가 중요하다. 정부는 사건이 터질 때마다 대책을 내놓지만 대부분은 이전의 대책들을 종합한 것이다. 따라서 중요한 것은 대책이 실효를 거둘 수 있도록 하는 정부의 실행의지이다. 또한 법률이 엄격하게 개정된다고 하더라도 시행령이나 시행규칙 개정 과정에서 얼마든지 완화될 소지가 있다. 정부는 법 취지가 훼손되지 않도록 하위규정을 만들어야 할 것이다.

4. 결 론

정보유출 사건이 계속되는 이유는 정보의 암호화, 내부자·외부자에 대한 인적보안 태만 등 기본을 지키지 않기 때문이다. 이 두 가지 원칙만 잘 지켜도 정보유출은 대부분 방지할 수 있을 것이다. 정부는 대책만 내 놓지 말고 대책이 실질적으로 효과를 거둘

수 있도록 실천의지를 보여줘야 할 것이다. 금융사는 보안 거버넌스(security governance) 전략으로 경영 차원에서 접근해야 하며 금융사 경영진의 근본적인 인식변화와 강력한 실행력이 뒷받침되어야 한다. 소비자도 자기정보결정권을 적극 활용해 정보주체로서의 권리강화에 힘써야 할 것이다. 정부, 기업, 소비자가 삼위일체가 되어 지금까지 무형자산인 신용을 이사회에 뿌리내리게 한 카드 산업의 추락으로 신용사회가 붕괴되지 않도록 최선의 노력을 다해야 할 것이다.

참고문헌

[1] 금융위, “신용카드업자 고객정보 유출관련 현황 및 대응 방안”, 보도자료, 2014.1.8.

[2] 박해욱, “보험사GA서도 개인정보 유출”, 서울경제신문, 2014.3.25.

[3] 이동현, “카드 가맹점 단말기 해킹해 고객정보 털었다.”, 한국일보, 2014.4.12.

[4] 강지원, “이번에 농협생명···자고나면 터지는 정보유출” , 한국일보, 2014.4.17.

[5] 금융위, “금융회사 고객정보 유출 재발 방지 대책”, 보도자료, 2014.1.22.

[6] 금융위, “개인정보 불법유통,활용차단 조치 시행”, 보도자료, 2014.1.24.

[7] 금융위, 기획재정부, 미래부, 안전행정부, 방송통신위원회, 금융감독원, “금융분야 개인정보 유출 재발방지 종합대책”, 보도자료, 2014,3.10

[8] 손철, “금융당국 IT 보안관리 총체적 부실”, 서울경제, 2014.4.18.

[9] 강지원, “족쇄 풀리는 카드 3사 - 600만 이탈고객 잡아라.”, 한국일보, 2014.5.12.

[10] 강지원, “금융사 3곳중 2곳 CISO 없어요”, 한국일보, 2014.4.14.

[11] 이호정, “KB금융지주, CEO 스코어 문제 제기후 CISO 제도 첫 개편”, The CEOScoreDaily, 2014.4.21.

[12] 박윤선, “다시 늘어난 카드 모집인”, 서울경제, 2014.4.11.

[13] 박준서, 이지훈 “대출중개업 초토화__올들어 대출모집인 절반 업계 떠나”, 한국경제, 2014.4.18.

[14] 김현희, “‘주민등록번호 암호화’ 개인정보보호법 개정_금융사 비상”, 파이낸셜 뉴스, 2014.3.2.

[15] 사설 , “금융권 암호화 늦출 일 아니다”, 디지털타임스, 2014.4.17.

[16] 앨런 케슬러, “개인정보유출 대재앙 막으려면”, 서울경제, 2014.5.7.

[저 자 소 개]

정 기 석 (Gi-seog Jeong)

1983년 2월 고려대학교 전자공학과 학사
1988년 8월 고려대학교 전자공학과 석사
1992년 8월 고려대학교 전자공학과 박사
현재 영동대학교 정보통신보안학과 교수

email : gsjeong@yd.ac.kr