금융거래와 개인신용정보의 보호

Protection of Personal Credit Information in the Cross-border Financial Transactions

박 훤 일*
(Park, Whon-Il)

〈차 례〉

주제어 : 개인신용정보, 비공개 개인정보, 프라이버시 지침, 개인식별정보, 개인정보 도용, 정보주체의 동의, 동의철회, personal credit information, nonpublic personal information, privacy guidelines, identity information, identity theft, consent, opt-out

Ⅰ. 머리말

최근 들어 개인신용정보(personal credit information)의 오·남용에 대한 금융소비자들의 우려가 고조되고 있다. 제3자가 피싱(phishing)[1]을 통하여 금융사기를 획책한다거나, 최근 국민은행이 고객들의 개인정보를 부주의로 유출시킨 사례[2]와 같이 고객정보가 부실하게 관리된다면 금전상의 피해를 볼 수 있기

* 경희대학교 법과대학 조교수/국제법무대학원 인터넷법무학과 주임교수, 법학박사.

1) 'phishing'이란 e-메일을 미끼로 인터넷의 바다에서 낚시질(fishing)하듯이 금융사기의 대상을 고르는 행위를 말한다. 'f'가 'ph'로 바뀐 것은 컴퓨터 해킹의 전통에 따른 것이다.

2) 국민은행은 2006년 3월 15일 자사 인터넷 홈페이지 회원 3000여 명에게 인터넷 복권을 안내하는 광고 메일을 보내면서 다른 고객 3만여 명의 신상정보가 담긴 첨부 파일

때문이다. 여기에는 자기가 원치 않는 불리한 신용정보가 금융기관들 사이에 유통되는 것도 포함된다. 온라인을 통한 전자상거래가 발달하려면 그 전제로서 소비자들이 안심하고 인터넷을 이용할 수 있어야 한다.

그러나 오늘날과 같은 정보화사회에서 개인신용정보를 감춰놓고만 있을 수 없는 노릇이다. 자신에게 유리한 신용정보는 널리 유통될수록 금융기관에서 신용을 얻거나 취업을 할 때 유리하다. 인터넷을 통한 금융거래가 널리 행해지고 있는 요즘에는 적극적으로 신용정보가 유통되어야만 금융기관으로서도 제대로 리스크관리를 할 수 있게 된다. 나아가 고객들의 신용상태와 성향을 파악하여 새로운 상품개발 및 마케팅에도 나설 수 있을 것이다.

이러한 사정은 국제금융거래에 있어서는 더욱 강조된다고 볼 수 있다. 예컨대 자신의 신용정보가 유출되어 해외에서 제3자가 자신 명의로 신용카드를 사용한다든가 자신의 은행계좌에서 자금을 빼내려 한다면 그 직접적인 피해를 입을 수 있을 뿐만 아니라 저하된 신용을 원상태로 회복하는 것도 심각한 문제가 아닐 수 없다.

본고는 국내 거주하는 외국인이 국내 A은행에 대출을 신청하였을 때 신청인의 본국 B신용정보회사(credit reporting agency: CRA)에 그의 신용정보를 요청하는 상황[3]을 가정한다. 본고는 이러한 관점에서 歐美의 주요국들이 개인신용정보를 보호하기 위하여 어떠한 법제를 갖추고 있으며, 이를 어떻게 운용하고 있는지 살펴보고자 한다. 이 과정에서 우리나라의 현행 「신용정보의 이용 및 보호에 관한 법률」(이하 “신용정보법”이라 함)에 개선을 요하는 사항은 무엇인지 알아보기로 한다.

을 함께 보냈다. 첨부 파일에는 고객의 이름과 주민등록번호, e-메일 주소 등이 상세하게 적혀 있었다. 중앙일보 2006.3.16; 4월 하순에는 온라인 게임 ‘리니지2’를 서비스하는 엔씨소프트사가 서울중앙지방법원으로부터 1인당 50만원을 지급하라는 손해배상 판결을 받았다. 법원은 “다수이용자를 대상으로 게임 서비스를 제공하고 수익을 얻는 업체는 이용자 개인정보를 보호하기 위해 특별한 주의의무를 부담해야 한다”고 밝혔다. 비록 실제 손해는 확인되지 않았지만 피고회사가 부주의하게 이용자들의 ID와 비밀번호를 암호화하지 않음으로써 개인정보가 유출될 우려가 있었고 이에 대하여 위자료를 지급하도록 한 것이다..

3) EU집행위가 제3국의 개인정보보호 수준을 평가하기 위하여 벨기에 나뮤르 소재 평화 노트르담대학교(FUNDP) 정보와 법 연구소(CRID)에 용역을 의뢰하였을 때 CRID가 취한 사례별 접근방법(case by case approach)의 하나로 채택되었던 사례 가운데 하나이다. 박훤일, 「EU 개인정보보호지침 준상호주의 이행방안 연구」, 한국정보보호진흥원 최종연구보고서: 개인정보연구01-02, 2001.11, 39면, 76～79면.

Ⅱ. 국제적인 개인신용정보보호의 현황

1. 국제적인 신용정보보호 규범

오늘날 금융기관을 포함한 많은 기업들은 제품·서비스를 보다 효율적으로 제공하고 급변하는 시장에서 경쟁력을 확보하기 위해 고객들의 개인정보를 수집하고 고객들의 프로파일(user profile)을 구축하는 데 주력하고 있다.[4] 그러나 이와 같은 기업들의 노력은 '消費者主權'(consumer sovereignty)의 시대에 자신의 개인정보를 스스로 통제하고 원치 않는 정보가 유통되는 것을 막으려는 이용자의 기본입장과 종종 충돌을 빚게 된다. 기업이나 개인이 개인정보의 보호를 소홀히 하여 발생하는 피해가 갈수록 증가하고 있다.[5] ID 도용 외에 데이터 사보타지, 개인정보의 유용 및 무단 거래까지 고려한다면 그 피해는 천문학적인 규모로 늘어날 것이다.

EU에서는 개인정보에 있어서 신용정보를 따로 구분하지 않지만 미국에서는 금융서비스현대화법(Financial Services Modernization Act of 1999, 일명 "Gramm-Leach-Bliley Act": GLBA)에서 이를 별도로 규정하여 보호하고 있다.[6]

2. 유럽연합(EU)

가. EU 개인정보보호지침

유럽에서는 1950년의 유럽인권협약[7]과 1981년의 유럽회의협약[8]에 이어 EU

4) 기업들이 고객의 개인정보를 수집하는 것은 고객들의 행태(action and behavior)에 관한 정보를 가급적 많이 수집하여 이를 데이터베이스화함으로써 다른 정보와 연계하여 고객들의 행동을 정확히 예측하기 위한 것이다. 심리학에서는 이를 '프로파일링'이라 하는데, 컴퓨터를 이용하면 방대한 데이터도 손쉽게 분석할 수 있다.

5) 미국의 경우 2003년 한 해 동안 990만명 이상이 ID를 도용 당한 사례가 있으며, 이로 인하여 기업들은 480억달러 가까운 손해를 입고 소비자들도 50억달러에 달하는 피해를 본 것으로 나타났다. 기업들은 ID 도용(identity theft)으로 평균 4,800달러, 소비자는 평균 500달러의 손해를 입은 셈이다. Sun Microsytems, *Privacy and Data Protection: Mitigating the Risks of Information Exposure, A Technical White Paper*, July 2004, p.1.

6) 신용정보 외에도 미국에서는 개인의 헬스케어정보(healthcare information)는 Health Information Portability and Accountability Act (HIPAA)에 의하여, 의약정보(pharmaceutical information)는 21 CFR part 11에 의하여 각각 별도의 보호를 받고 있다.

7) 「인권 및 기본적 자유의 보호를 위한 유럽협약」(European Convention for the Protection

가 1995년 EU 개인정보보호지침(Directive 95/46/EC, 이하 “EU지침”이라 함)[9]을 채택함에 따라 동 지침은 개인정보의 개념이나 그 보호기준에 있어서 사실상 국제기준(global standards)으로서 자리매김하게 되었다.

EU지침은 역내에서 개인정보를 취급하는 경우에 항상 적용되는 것은 아니다. 동 지침에 의하면 개인정보의 처리를 전부 또는 일부 자동화 수단(automatic means)으로 하는 경우, 또는 개인정보를 자동화 수단 이외의 방법으로 처리하더라도 그것이 파일링 시스템의 일부를 구성하거나 구성할 의도로 처리되는 경우에도 적용된다. 즉 개인정보를 컴퓨터로 처리하거나 手作業(manual)으로 하더라도 개인에 관하여 일정 기준에 따라 구조화된 파일링 시스템을 갖추게 되면 EU지침이 적용되는 것이다.[10] 그러나 공동체법의 적용범위 밖에서 개인정보가 처리되는 경우, 예컨대 공공의 안전, 방위, 국가안보, 형사법 분야에서의 국가활동에 관하여 처리작업이 이루어지는 경우, 또한 자연인에 의한 순수하게 개인적이거나 가정내 활동 중에 처리되는 경우에는 개인정보보호지침이 적용되지 아니한다.[11]

EU지침에 있어서 개인정보의 내용은 정보기술의 발달에 발맞추어 개인을 알아볼 수 있는 부호・문자・음성・음향・영상 등의 모든 정보를 망라한다. 신용정보를 특별히 구분하지 아니한다. 그러나 보도의 목적이나, 문학적 또는 예술적 표현의 목적으로 행하여지는 음성 및 영상 정보의 처리(특히 시청각 분

---

of Human Rights and Fundamental Freedoms, ECHR). 유엔인권조약의 영향을 받아 로마 외교회의에서 1950년에 채택되었고 1953년 9월 3일 발효되었다. 동구권의 체제전환 이후 러시아까지 망라한 40여개의 거의 모든 유럽 국가들이 이에 가입해 있다. <http://www.coe.fr/tablconv/5t.htm>

8) 「개인정보의 자동처리와 관련된 개인의 보호를 위한 유럽회의 협약」(Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, Euro. T.S. No.108: CoE 108). 개인정보보호에 관한 EU지침 외의 유력한 국제조약으로서 그 비준국은 15개 EU 회원국과, 노르웨이・아이슬란드 등의 유럽경제지역협정(European Economic Agreement: EEA) 체약국 및 슬로베니아, 헝가리, 스위스 등의 제3국이다.

9) 「개인정보의 처리 및 자유로운 전송에 관하여 개인을 보호하는 유럽의회와 집행위원회의 지침」(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data). 각 회원국은 3년 내에 동 지침에 입각한 국내입법을 해야 하므로 이미 개인정보법제를 시행하던 나라들도 이에 맞춰 법률을 개정하여야 했으며, 신입 회원국들도 다른 나라의 법제를 모방함으로써 이 기준에 부응하였다. 그 결과 2003년 아일랜드와 프랑스를 마지막으로 EU지침의 역내 입법작업이 완료되었다.

10) EU지침 전문 27) 및 제2조(정의) (c)호.

11) EU지침 제3조(범위) 참조.

야)에 있어서는, 개인정보의 처리와 표현의 자유와 관련하여, 표현의 자유와 프라이버시권을 조화시킬 필요가 있는 경우에 한해 例外가 인정된다.[12)]

EU는 신용정보를 포함한 개인정보의 비밀을 지키도록 하되, 정보주체가 자신의 무슨 정보가 수집되고 누가 이를 어떻게 이용하는지, 어디에 보관하는지, 어떻게 오류를 수정하고 갱신이 되는지, 어떻게 삭제할 수 있는지 同意 및 동의 철회 등의 절차를 통해 이를 통제할 수 있도록 하였다. 그러므로 개인정보가 적절한 수준으로 보호(adequate level of data protection)되지 않는 域外[13)] 제3국에 대하여는 회원국의 개인정보 감독기구가 정보의 이전을 금지하고 있다.

나. 제3국으로의 정보이전이 허용되는 경우

그러나 자유로운 정보유통을 촉진하기 위하여 제3국의 법제가 개인정보를 적절히 보호하지 못하더라도 개인정보보호를 위한 각종 안전조치(safeguards)가 취해져 있는 경우에는 정보의 이전을 허용한다. 현재 EU지침에 의거하여 집행위원회(Commission)가 인정하고 있는 안전조치로는 ① 미국과의 정보교류에 있어서 미국 연방거래위원회(Federal Trade Commission: FTC)의 감독 하에 자율규제 방식으로 실시하는 세이프하버 원칙(Safe Harbor Principles), ② 집행위원회가 승인한 표준계약서(ad hoc/model contract), ③ 유럽에 기반을 둔 다국적기업의 경우 EU지침에 맞게 프라이버시 정책을 운영하는 구속력 있는 기업규칙(Binding Corporate Rules: BCRs) 등이 있다.[14)] 현재 이미 적절한 수준의 개인정보보호가 이루어지고 있는 나라들은 이른바 '화이트 리스트'[15)]에 올려놓고 이들 나라에 대하여는 별도의 조치 없이 개인정보를 이전할 수 있도록 하고 있다.

冒頭에 상정한 케이스에서 신청인이 EU 회원국의 시민이라고 하자. 국내 A은행은 그의 대출신청을 받고 EU 회원국 소재 B신용정보회사에 신청인의 신용정보를 요청하여야 할 것이다. 한국은 아직 EU지침 상의 화이트 리스트에

12) EU지침 제2조(정의) (a)호 및 전문 37), 유럽회의(CoE) 협약 제10조 참조.

13) EU 개인정보보호지침은 EU 회원국은 물론 유럽회의협약(Council of Europe Convention 108)을 체결한 유럽경제지역(European Economic Area: EEA)의 3개 가맹국 아이슬란드, 리히텐슈타인, 노르웨이를 대상으로 한다.

14) 이에 관한 자세한 해설은 박훤일, "개인정보의 보호를 위한 안전조치 - 개인정보보호 기업규칙(BCRs)을 중심으로",「경희법학」제40권 2호, 2005.12, 177~187면 참조.

15) EU가 EU지침 제25조 제1항과 관련하여 개인정보가 적절한 수준으로 보호되고 있다고 인정한 나라는 스위스(1999), 헝가리(1999), 미국(세이프하버 조건부 2000.7), 캐나다(2001), 아르헨티나(2002), 건지(Guernsey 2003), 만섬(Isle of Man 2003) 등이다.

올라 있지 않고 국내 A은행이 EU에서 인정하는 BCRs을 작성하지도 않았으므로 A은행과 B회사 간에 EU집행위에서 승인한 표준계약서에 의하여 신청인의 신용정보를 주고받거나, 신청인의 사전동의를 얻어 A은행이 B회사로부터 해당 신용정보를 받아와야 할 것이다.

3. 미 국

가. 개 요

미국에서는 프라이버시 내지 개인정보의 보호를 지역이나 산업 별로 보호하는 것이 특색이다. 신용정보에 국한시켜 본다면 「사베인스-옥슬리법(Sarbanes-Oxley Act: Sarbox), 「그람-리치-블라일리법(GLBA)」, 「신용보고법(Fair Credit Reporting Act: FCRA)」 등이 신용정보에 대하여 규율하고 있다.

엔론 사태 이후 기업회계제도를 개혁하기 위해 제정된 사베인스-옥슬리법에서는 공개법인의 최고경영책임자(CEO)와 최고재무책임자(CFO)가 당해 법인의 신용정보의 정확성 및 監査가능성(auditability)을 입증하도록 하였다. 그러므로 CEO와 CFO는 누가 무슨 신용정보를 열람하고자 하는지 파악하고 있어야 한다.[16]

개인신용정보의 보호에 관한 법률은 GLBA[17]이다. 이 법은 본래 은행의 증권업무 취급제한을 폐지하고 은행과 증권사·보험사의 합병을 허용하기로 한 법률로 유명하거니와, 이에 따른 개인신용정보의 안전한 보관, 정보공유에 관한 금융기관 정책의 통지, 금융소비자의 정보공유에 대한 거부권을 규정할 필요가 있었다.[18] 따라서 GLBA는 기존 FCRA 등의 프라이버시 규정들을 보완하

16) 이에 관한 자세한 내용은 <http://www.aicpa.org/info/sarbanes_oxley_summary.htm> 참조. Sun Microsystems, op.cit., p.9.

17) GLBA는 1932년 이래 은행업과 증권·보험업을 구분해온 글래스-스티걸법을 폐지한 금융서비스현대화법으로 잘 알려져 있는데 개인신용정보보호 규정은 제5장(Title V)에 규정되어 있으며, 15 U.S.C. §§6801-6810에 편찬되어 있다.

18) 법안이 심의될 무렵 금융기관들이 고객정보를 유용하여 사회적으로 물의를 빚은 사건들이 잇달았다. 1997년 캘리포니아주의 차터 퍼시픽 뱅크는 성인 웹사이트에 수백만 명의 신용카드번호를 팔아 넘겨 일부 고객들은 보지도 않은 인터넷 포르노 사이트 접속료를 내라는 독촉을 받았다. 2000년 FTC는 이 웹사이트 회사에 대해 3,750만달러의 배상을 청구하여 승소판결을 받았다. 1998년 네이션즈뱅크는 고객정보를 증권자회사와 공유하여 고객들이 위험이 높은 증권에 투자하게 하는 바람에 많은 손실을 입혔고 이 은행은 결국 수백만달러의 벌금을 물어야 했다.

는 동시에 넓은 의미의 금융기관들(financial institutions)[19]에 대하여 개인신용정보보호의 의무를 부과하는 기준을 마련하였다는 데 의의가 있다.[20] GLBA 가이드라인에 의하면 금융기관들은 문서로 된 보안계획(written information security plan)을 수립하고, 책임자를 임명해야 하며, 고객들의 신용정보에 대한 위험을 평가하고 수시로 안전조치를 테스트하고 모니터링해야 한다. 2003년 연방의회는 그해 말로 끝나는 FCRA의 효력을 연장한 새 법(Fair and Accurate Credit Transactions Act: FACTA, Public Law 108-159)을 제정하여 명의도용(identity theft)과 같은 개인정보의 유출·도용에 대하여 금융기관에 한층 강화된 개인신용정보 보호의무를 부과하였다.

나. 非公開 個人情報의 처리

GLBA에서 핵심이 되는 개념은 '非公開 개인정보(nonpublic personal information: NPI)'이다. 동법상의 定義에 의하면 금융소비자가 금융기관에 거래신청 시 제공하거나, 당해 소비자와의 거래 또는 그를 위한 서비스의 결과로서 생기는 것 또는 금융기관이 달리 취득한 것으로서, 개인을 식별할 수 있는 금융상의 정보(personally identifiable financial information)를 말한다.[21]

그러나 개인 이름이라 해도 그 특정성 여부와 일반적인 입수 가능성을 고려해 개인정보로서 규제 대상이 될 수도 있고 안 될 수도 있다. 예컨대 어떤 사람이 특정 금융기관의 고객이라는 정보는 일반적으로 비공개 개인정보이지만, 공무소에 보관된 등기부에 그 사실이 기재되어 있다면 공개된 정보로서 입수 가능한 것이다.

비공개 개인정보의 취급에 있어서 GLBA는 신용정보의 보호를 위한 안전조치(Safeguard Rules)를 요구하고 있는데[22] 이에 의하면, ① 프라이버시 지침이

---

19) GLBA에서 금융기관이란 은행지주회사법(Bank Holding Company Act of 1956) 상의 금융기관인 은행, 신용협동조합, 저축기관은 물론 증권거래위원회(SEC)와 상품선물거래위원회(CFTC), 연방거래위원회(FTC)의 관할에 속하는 기관(예: 증권회사, 선물회사, 채권추심회사, 여신전문금융회사, 신용정보회사, 감정평가사, 세무사 등)도 포함한다. 보험회사는 연방법이 아닌 州法의 규율을 받는데 역시 GLBA의 프라이버시 보호 규정의 적용을 받고 있다. GLBA 시행 당시 개인의 신용문제를 다루는 변호사도 이에 포함되는 것으로 이해되었으나 워싱턴DC의 항소법원에서 이를 배척하였다.

20) 부기덕, "금융가산책: 개인정보보호법 제정과 금융기관의 대응", 「대은 경제리뷰」, 대구은행, 2005, 73면.

21) GLBA Sec.509(4)(A). Robert H. Ledig, "Gramm-Leach-Bliley Act Financial Privacy Provisions: The Federal Government Imposes Broad Requirements to Address Consumer Privacy Concerns", Fried Frank. <http://www.ffhsj.com/bancmail/bmarts/ecdp_art.htm>

나 실무관행을 기재한 통지의무를 부담지우고, ② 관련이 없는 제3자(unaffiliated third parties)와의 정보공유(information sharing)에 대하여 사전거부권(right to opt-out)을 부여하며, ③ 마케팅 목적으로 계좌번호 등을 제3자에 제공하는 것을 금지하고 있다.

즉, 금융기관은 프라이버시에 관한 지침(Privacy Guidelines)을 정하는 가운데 프라이버시 지침이나 실무관행이 정확히 반영된 통지(privacy notice)를 ① 계속적인 거래관계(ongoing relationship)가 있는 개인고객에 대해서는 거래관계가 발생한 때와 그 후 적어도 연 1회, ② 계속적인 거래관계가 없는 개인에 대해서는 그 사람의 비공개 개인정보를 관련이 없는 제3자에 제공하기 전에 송부해야 한다. 이미 통지한 것과 다른 정보의 수집·제공을 행하는 경우에는 사전에 수정 통지를 보내야 한다. 그러나 계속적인 거래관계가 종료하는 개인에게는 새로 年次통지(annual notice)를 할 필요가 없다. 프라이버시 통지는 ① 수집하는 비공개 개인정보, ② 제공하고자 하는 비공개 개인정보, ③ 비공개 개인정보를 제공하는 관련회사(affiliated companies)나 관련이 없는 제3자 등으로 구분되어 있다.

다음으로 관련이 없는 제3자와의 정보공유에 있어서 선택권은 어떻게 부여하는가. GLBA에 의하면 금융기관이 관련이 없는 제3자에게 비공개 개인정보(NPI)를 제공하거나 공유하는 경우에는 앞서 말한 프라이버시 통지 요건을 갖추어야 한다. 그리고 본인에 대하여 이를 사전에 거부(opt-out)할 수 있는 기회를 제공하여야 한다. 구체적으로 살펴보면, 금융기관이 관련이 없는 제3자와 비공개 개인정보를 공유하고자 하는 경우, ① 각 정보주체에 대하여 NPI가 관련이 없는 제3자에게 제공될 것임을 서면, 전자적 방법 기타 관련규정이 허용하는 방법으로 알리고, ② 정보주체가 NPI가 제공되기 전에 이를 거부할 수 있는 30일 이상의 시간여유를 주고, ③ 본인이 사전거부권을 행사하지 않아야 한다. 즉, 사전거부권의 통지에서는 ① 금융기관이 관련이 없는 제3자와 정보를 공유할 수 있다는 점, ② 고객에게 사전거부할 권리가 있다는 점, 그리고 ③ 사전거부권의 행사방법에 대해서 알기 쉽게 설명하여야 한다.

통지의 송부, 충분한 오프트-아웃[23] 권리행사 기회의 제공, 권리의 행사 없

22) GLBA는 FRB, SEC, FTC 등 각 금융기관 감독당국에 대하여 동법 시행에 필요한 사항을 규정하도록 함에 따라 FRB는 2000년 11월 「규정 P」(Regulation P: Privacy of Consumer Financial Information)를 제정하였다. Andrew J. Morris, Brian W. Smith, Kimberly Kiefer and Cregory S. Feder, "4.06 Financial Institutions: Agency and Industry Initiatives", *E-Commerce Financial Products And Services,* ALM Properties, Inc., 2005.

음의 세 가지 요건이 모두 충족되어야 관련이 없는 제3자와의 정보공유가 가능하기 때문에, 단순히 프라이버시 통지를 송부하고 즉각적인 오프트-아웃의 의사표시가 없음을 근거로 제3자에게 고객의 개인정보를 제공할 수 있는 것은 아니다. 여기에는 금융기관의 실무수요를 고려한 몇 가지 예외(exceptions) 규정이 있는데, ① 금융기관이 정보처리를 아웃소싱하고 있는 경우, ② 타 금융기관과의 공동마케팅을 추진하는 경우, ③ 본인이 요구하는 거래를 수행하기 위해 불가피한 경우, ④ 부정행위나 무권한 거래(unauthorized transactions)를 방지하기 위한 경우, ⑤ 금융기관의 리스크관리에 필요한 경우 등이다. 프라이버시 통지와 관련하여 ①, ②의 경우는 당초의 프라이버시 통지가 필요하지만, ③, ④, ⑤의 경우에는 통지를 요하지 아니한다.

고객이 오프트-아웃의 의사표시를 한 경우 금융기관은 신속히 그에 응하여야 한다. 본인의 의사표시는 당초의 이사표시 기회 이후에도 언제든지 가능하며, 본인이 수정・철회를 하지 않는 한 유효하다. GLBA에서는 관련회사간의 비공개 개인정보의 공유에 관하여 규정하지 않고 있기 때문에 이에 관하여는 기존 FCRA의 규정이 그대로 적용된다. 다만, 소비자에게는 관련회사와의 정보공유를 금지할 수 있는 권한이 없어 이러한 계열사간의 정보거래 명목으로 그룹 내부에서 신용정보의 거래가 이루어지는 것(corporate family trading)은 막을 수 없다.

그리고 금융기관이 신용정보회사를 제외한,[24] 관련이 없는 제3자에 대하여 텔레마케팅 등의 목적으로 개인의 계좌번호, 신용카드번호 등의 접근매체(access code)를 제공하는 것은 금지된다. 다만, 접근매체가 암호화되어 있는 경우에는 그 해독방법이 제공되지 않는 한 금지의 대상이 아니다. 이 규정의 취지는 정보를 입수한 외부업자가 본인에게 무단으로 대금 등을 청구하는 것을 방지하기 위한 것이므로, 이는 제3자와의 비공개 개인정보의 공유에 관해서 본인이 오프트-아웃하지 않은 경우뿐만 아니라 본인의 동의가 있는 경우에도 해

23) 'Opt-out'이란 제시되어 있는 대안을 거부하거나 동의를 철회한다는 의미이다. 거래하는 금융기관으로부터 "귀하의 개인정보를 제3자에게 제공하겠다"는 통지를 받았을 때 이를 거부하는 것을 말하며, 당해 금융기관은 수신거부 또는 동의철회를 위한 무료전화서비스 등을 명시하여야 한다. 오프트-아웃은 사후적으로만 할 수 있는 게 아니고, 예컨대 스패머 명단을 지정하는 경우와 같이 사전적으로도 거부할 수 있다. 우리나라 정보통신망법 제50조에도 오프트-아웃 규정이 있다.

24) GLBA에 의하면 금융기관은 영업을 양도하거나, 법령을 준수하기 위하여, 또는 고객이 요구하는 거래를 하는 데 필요한 경우 고객의 신용정보를 신용평가회사나 금융감독기관에 제공할 수 있다.

당된다.

끝으로 GLBA에서 엄격히 금지하고 형사처벌까지 하는 것으로 이른바 '프리텍스팅(pretexting)'이 있다. 이것은 감독기관, 사회복지사, 고용주 등으로 거짓 가장하거나 복권당첨, 보험금지급 등을 핑계 대고 개인정보를 수집하는 행위를 말한다. GLBA는 금융기관으로부터 또는 금융기관의 고객에 대하여 고객정보를 수집하기 위하여 허위, 가공 또는 사기적인 말을 하거나 서류를 제시하는 것, 또는 위·변조 문서, 절취한 문서를 이용하는 것을 금지하고 있다. 타인에게 이러한 행위를 부탁하는 것도 금지된다.

다. 各州 및 금융기관의 동향

GLBA의 개인신용보호 규정이 2001년 7월부터 시행되었으나, 캘리포니아주에서는 이보다 더욱 엄격한 금융 프라이버시 보호규정을 시행하고 있다. 예컨대 2003년 8월 캘리포니아주 1386호 법(California Senate Bill 1386)에 의하면 캘리포니아주 주민의 개인정보를 분실한 법인, 조직은 캘리포니아주에서 유통되는 미디어(major statewide media)에 의한 통지문을 보내 그 고객들에게 주의를 촉구하여야 한다. 여기서 개인정보는 성명(last name and first initial 포함), 운전면허증 번호, 사회보장번호, 신용카드번호, 은행계좌번호 등이 이에 해당한다. 미국 기업 치고 캘리포니아 주민을 고객으로 하지 않는 곳은 없기 때문에 전국적인 적용 가능성을 갖고 있다고 볼 수 있다.

인터넷을 통해 금융상품·서비스를 제공하는 대부분의 미국 은행들은 자사의 홈페이지에 프라이버시 정책을 게시하고 있다. 웹(web) 사이트의 게시를 통해 고객의 동의를 얻을 수 있다면 금융기관들이 프라이버시 규정 준수를 위한 부담이 크게 줄어들 것이다. 각 은행의 프라이버시 정책을 보면, 개인고객을 대상으로 영업을 하는 데 따른 일률적인 지침을 정하고 있는 바, 뱅크오브아메리카(Bank of America)의 경우 법률규제 이상의 개인정보보호를 자발적으로 실시하고 있다. 정보수집·이용의 목적에 있어서 대부분 금융그룹에 의한 서비스의 제공이나 고객 니즈의 충족 등 일반적인 표현에 그쳐 있다.[25]

라. GLBA에 의한 신용정보의 공유

冒頭에 상정한 케이스에서 신청인의 대출신청을 받은 국내 A은행이 美國系

25) 부기덕, 전게 논문, 76면.

은행일 경우 GLBA에 의하여 동일 은행지주회사 산하의 계열사 간에는 신용정보의 공유가 가능하므로 미국내 본사로부터 신청인의 신용정보를 용이하게 입수할 수 있을 것이다. 그밖의 경우에는 A은행이 신청인의 사전동의를 얻어 미국내 C신용정보회사로부터 신청인의 신용정보를 구입하여야 할 것이다.

Ⅲ. 개인신용정보 보호법제의 개선 움직임

1. 규범적 측면

미국에서는 GLBA만 가지고는 개인신용정보의 보호나 ID 도용에 한계가 있다고 보고 연방의회 차원에서 그 개선방안을 마련하고 있다. 대표적인 문제점은 GLBA가 소비자에게 정보공유에 대한 사전거부권을 부여하고 있지만 이를 행사하기가 쉽지 않으므로 그룹 내부에서 고객정보를 공유하는 것이 당연시되고 있다는 것이다.

관련기관과의 정보공유(affiliate sharing)에 대해서는 소비자가 이를 통제할 수 없게 되어 있어 은행이 합병을 통해 인수한, 금융업과 전혀 관계없는 계열사에 고객정보를 이전하더라도 이를 저지할 방도가 없다.[26] 더욱이 금융기관이 소비자에게 通知를 하는 것에 명확성이나 투명성이 결여되어 있어도[27] 또는 GLBA상의 例外에 해당한다고 우기더라도 이를 견제할 수단이 전혀 없다. GLBA 위반행위에 대하여는 피해를 입은 소비자가 직접 救濟를 청구할 수 없고, FRB, FDIC, FTC와 같은 연방감독기구만이 소송을 제기할 수 있게 한 것도 동법의 實效性을 떨어뜨리고 있다.[28]

최근 들어 개인정보 침해사고가 빈발하고 있음에도 정보처리업무에 대한 전국적으로 통일된 기준이 없고 특히 소매업자나 제3의 정보처리업자에 대하여는 규제가 미치지 않는 문제점이 지적되었다. 2005년 10월 하원에서 발의된 「금융정보보호법안(proposed Financial Information Protection Act, H.R. 3997)」은 이

26) Electronic Privacy Information Center (EPIC), "The Gramm-Leach-Bliley Act," January 2005. <http://www.epic.org/privacy/glba/>

27) GLBA에 의하면, 금융기관이 소비자에게 그의 개인정보가 공유된다는 것을 알려야 하지만, 누가 무슨 목적으로 그 정보를 이용하는지에 대해서는 통지하지 않아도 된다.

28) EPIC, *op.cit.*

문제를 해결하기 위한 법안이다. 동 법안은 GLBA 및 FCRA의 개인신용정보 안전조치의무(data safeguards requirements)를 확대함으로써 소비자의 금융정보(financial account) 또는 개인식별정보(identity information)를 보유·유지하는 모든 기업에 통일적으로 적용되는 기준을 정하는 것을 목적으로 한다.[29] 현재 하원 금융서비스위원회에 계류 중(pending)에 있는데, 2006년 중 하원 전체회의에 회부되고 상원과도 조율을 거쳐야 법률로서 효력을 발생하게 된다.

동 법안에서는 어느 소비자의 민감한 정보(sensitive consumer information)가 유출되어 ID 도용(identity theft)이나 金融詐欺(account fraud)가 일어날 우려가 있을 때 즉시 통지를 하도록 하고 있다. 동 법안은 GLBA처럼 금융기관만을 대상으로 하거나 FCRA같이 신용보고서만을 규율하지 아니한다. 이는 어느 기업이든지 개인정보를 입수하여 명의도용, 금융사기 기타 범죄에 이용하는 것을 방지하기 위한 것이다. 금융소비자들로 하여금 자신의 개인정보가 침해받을 가능성이 있다는 사실을 접하였을 때 그에 대처할 수 있게 하고 실제로 침해사고가 발생한 때에는 신용기록(credit history)을 정정할 수 있도록 할 방침이다.

금융정보보호법안은 골자는 다음과 같다.

① 모든 기업은 개인정보보호 정책을 마련하여야 하며, 소비자에 관한 민감한 금융정보의 보안 및 비밀유지에 필요한 절차를 갖추어야 한다.

② 기업은 개인정보가 침해되었을 때에는 즉각 조사를 벌여야 한다.

③ 정보보안이 침해되어 소비자들에게 손해나 불편을 끼쳤다면 기업은 수사기관, 해당 감독기관(regulator) 기타 거래 상으로 연결되어 있는 다른 기업(other business in the transaction chain)에 통지하여야 한다. 소비자들이 금융사기의 피해를 입을 수 있는 경우에는 해당 소비자들에게 우편(uniform mailing)으로 통지하고 無償으로 신용조사 서비스(free credit-file monitoring)를 받을 수 있도록 하여야 한다.

요컨대 민감한 소비자정보를 보호하기 위한 전국적인 기준을 설정함으로써 정보의 침해를 방지하고, 기관에 대하여는 소비자들에게 정보가 침해되어 ID 도용 등에 이용될 수 있음을 통지하도록 하고 있다. 민감한 식별정보(sensitive identity information)의 침해 통지를 받은 소비자들에 대하여는 당해 기관이 무

29) 미국 하원 금융서비스위원회의 2006.3.17자 보도자료, “Committee Advances Stringent Data Security Measure, 48-17” <http://financialservices.house.gov/News.asp?FormMode=release&ID=775>

료로 6개월 간의 신용조사 서비스(nationwide credit monitoring service)를 제공하여야 한다.

동 법안은 개인정보 침해위험이 있는 소비자들에게 무료 신용조회 서비스를 해주는 것이 특색이다. 이를 통하여 기업들이 민감한 정보를 주의하여 보호하도록 하는 한편 소비자들도 자신의 정보가 침해받지 않도록 하는 등 균형을 이루는 데 역점을 두고 있다고 할 수 있다.

2. 기술적 측면

오늘날 각국의 개인정보보호 법제를 살펴보면 역사적 배경이나 정보기술 수준에 따라 개인정보보호 정책과 기준이 다양하게 나타남을 알 수 있다. 유럽 특히 EU에서는 EU지침을 기준으로 통일적인 개인정보보호 입법을 하고 프라이버시에 대한 권리를 기본권으로 보호한다. 이에 비하여 미국에서는 9·11 테러 사건 이후 상황이 크게 달라지기는 하였지만, 전통적으로 市場중심적인 정책을 취하여 당사자들이 자율적으로 개인정보를 보호하도록 하였다. 최근에는 정보기술의 발달에 따라 기술적으로 개인정보보호의 목적을 달성할 수 있다는 技術중심적 접근방법(technology-oriented approach)이 관련법령을 고치지 않아도 된다는 이점 때문에 주목을 받고 있다.

관련기업이 기술적인 해결을 도모할 때에는 다음 사항에 유의하여야 한다.[30]

① 고객의 신뢰(consumer confidence)를 얻을 수 있도록 ID 도용, 사기, 오·남용으로 개인정보를 보호할 수 있어야 한다.

② 직원이 개인정보를 비롯한 고객들의 데이터베이스에 접속하는 것은 '알 필요'가 있는 경우(on a "need to know" basis)에 한함으로써 기업의 위험(business exposure)을 줄인다. 예컨대 대고객 서비스 담당자는 재고정보를 열람할 필요가 없는 것이다.

③ 고객정보의 정확성(data integrity)을 실시간으로 유지할 수 있는 시스템을 개발하고, 보다 안전하고 간편한 방법으로 고객정보를 제공하고 정정할 수 있게 하여 경쟁의 우위(competitive advantage)를 확보하도록 한다.

④ 누가 언제 무슨 정보를 열람하였는지 기록을 해둠으로써 보안 프로그램을 언제든지 검사할 수 있게 하는 등 관련법령을 준수(compliance)하도록 한다.

30) Sun Microsystems, *op.cit.*, pp.6-7.

개인정보의 보호에 있어서는 개인정보의 수집, 관리, 열람, 동의 등과 관련된 식별정보의 관리(identity management)가 중심이 된다.[31] 그 내용은 해당 소프트웨어를 개발하는 회사에 따라 다르지만 대체로 식별정보의 관리·운영에 관한 일련의 행동을 규정한 User Provisioning, 기업별로 특수한 속성을 고려하여 프로파일 데이터의 정확성과 일관성을 보장하는 Profile Management, 그리고 데이터에 대한 권한 있는 열람 및 보안상의 통제에 관하여 정한 Access Management와 Password Management, 각종 규제를 준수할 수 있도록 식별정보의 구조(identity infrastructure)를 확정하는 Directory Management가 있다. 사고가 발생하였을 때 그 원인을 규명하고 대책을 마련할 수 있도록 접속기록(log records)을 보존하는 등 검사에 대비한 Audit & Reporting도 필수적이라 하겠다.

정보기술이 크게 발달한 오늘날에는 인터넷상으로 개인정보를 수집하고 관리하는 경우가 많으므로 그에 적합한 보안대책을 강구함으로써 과도한 위험에 노출되지 않도록 하고 위험을 줄여나가야 할 것이다.

Ⅳ. 우리나라 신용정보법에 대한 시사점

1. 문제점의 검토

우리나라에서는 신용정보가 다른 개인정보[32]와는 달리 신용정보법과 「금융실명거래 및 비밀보장에 관한 법률」, 금융지주회사법 등[33]에 의하여 규율을 받으며 주무부처도 행정자치부나 정보통신부가 아닌 재정경제부로 되어 있다. 이것은 신용정보법이 개인은 물론 법인의 신용정보까지 대상으로 하고, 신용

31) *Ibid.,* pp.11-13.

32) 민간부문에서의 개인정보보호에 관한 일반적인 규정을 두고 있는 「정보통신망 이용촉진 및 정보보호등에 관한 법률」(이하 "정통망법"이라 함)에 의하면 "개인정보"라 함은 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다(동법 제2조 1항 6호).

33) 이밖에 법령으로서의 효력을 갖는 것은 아니지만 금융감독원이 2005년 11월 공표한 「금융회사 등의 개인신용정보관리·보호 모범규준(Best Practice)」이 있다. 신용정보업자 등은 신용정보법 제20조 1항에 의하여 신용정보의 수집, 처리 및 이용 등에 대하여 금융감독위원회가 정하는 바에 따라 내부관리규정을 마련해야 한다.

정보를 중심으로 하는 신용조회·신용조사·채권추심·신용평가 등의 업무를 규율하고 있는 데다 민간부문의 개인정보 보호입법(정통망법)보다 먼저 제정된 것에 기인한 것으로 보인다. 다만, 신용정보의 정의가 신용정보법에서는 "금융거래 등 상거래에 있어서 거래상대방에 대한 식별·신용도·신용거래능력 등의 판단을 위하여 필요로 하는 정보로서 대통령령이 정하는 정보"(동법 제2조 1호)라고 하면서, 신용정보법 시행령에서는 신용정보주체의 식별정보(identity information)로서 일반적인 개인정보(동법 시행령 제2조 1항 1호에서 법인의 정보를 제외한 것) 외에 신용거래정보(동조 동항 2호), 거래능력정보(4호), 불량 신용거래정보(3호), 공공기관이 보유하는 신용정보(5호)까지 망라하고 있다.

그런데 개인의 신용정보는 금융거래는 물론 취업이나 주택임대차 등 경제생활 전반에 중요한 영향을 미치게 되므로 다른 개인정보보다 훨씬 민감하고 그만큼 중요한 보호대상이라고 할 수 있다. 다른 한편으로는 신용상태를 잘 모르는 개인과 거래하는 금융기관이나 당사자로서는 상대방의 정확한 신용정보를 파악하는 것이야말로 거래의 성패를 좌우하고 보유자산의 건전성을 결정짓는 중요한 요소가 아닐 수 없다. 그러므로 오늘날 개인정보보호의 국제적 기준(global standards)이 되고 있는 OECD의 프라이버시 8원칙[34]이 개인신용정보에도 당연히 적용된다.

冒頭에 제시한 사례에서 보듯이 어느 개인이 자신의 신용정보에 관하여 우려하는 것은 자신도 모르는 사이에 부정확한 정보가 이리저리 유통되는 것이라 할 수 있다. 자신의 신용정보가 정확하게 유지되고 누구에게 어떠한 목적으로 제공되는지 통제할 수 있다면 자신에 관한 유리한 정보는 보다 널리 유통되어 경제생활을 이롭게 할 수 있기를 기대할 것이다.

이러한 견지에서 우리나라에서 개인신용정보를 둘러싸고 대두되는 문제는 다음 세 가지로 요약할 수 있다.

첫째, 신용정보법이 보호해야 하는 신용정보의 범위는 어디까지인가. 이 문제는 미국의 비공개 개인정보(NPI)와 비교 검토를 요한다.

---

34) OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data(프라이버시 보호 및 개인정보의 국제적 유통에 관한 지침)에서 설정한 ① 수집제한(collection limitation)의 원칙, ② 정보정확성(data quality)의 원칙, ③ 목적구체성(purpose specification)의 원칙, ④ 이용제한(use limitation)의 원칙, ⑤ 안전성확보(security safeguards)의 원칙, ⑥ 공개(openness)의 원칙, ⑦ 개인참여(individual participation)의 원칙, ⑧ 책임(accountability) 등 8개 원칙을 말한다.

둘째, 정확한 신용정보의 유통을 어느 정도까지 허용할 것인가. 이는 금융기관 자산의 건전성(capital adequacy), 업무의 효율성(efficiency) 제고와, 신용정보의 유통으로 인하여 유·불리를 입게 될 신용정보주체의 참여(individual participation)의 원칙간에 어떻게 균형을 이룰 것인가 하는 문제라 하겠다.

셋째, 신용정보의 침해에 대하여는 어떻게 구제할 것인가. 이는 침해를 야기한 자의 책임범위와 정보주체의 청구권에 관한 문제라 할 수 있다.

2. 신용정보의 범위와 보호의 정도

신용정보가 국제적으로 널리 유통되고 있는 오늘날 우리나라에만 독특하게 신용정보의 개념을 정의할 필요가 없으며,[35] 그렇게 해서도 안될 것이다. EU에서 개인의 신용정보를 특별히 규정하지 않고 이를 민감한 개인정보로 분류하는 것을 보면 우리나라 신용정보법 및 동법 시행령에 규정되어 있는 개념은 일반적인 식별정보와 그와 연결될 수 있는 각종 신용 및 금융거래에 관한 정보를 例示한 것이라 할 수 있다.

보다 중요한 문제는 이러한 개인의 신용과 관련된 민감한 개인정보를 어떻게 취급하고 관리할 것인가 하는 것이다. 다시 말해서 미국에서와 같이 비공개 정보로 국한할 것인가 하는 문제이다. 미국에서는 GLBA의 입법연혁과 그 취지에 비추어 민감한 신용정보를 비공개 정보로 국한하고, 법원이나 행정청 등 공공기관이 보유하고 있는 신용정보나 금융기관이 자체적으로 수집한 정보는 보호대상에서 제외하였다.[36] 앞서 말한 바와 같이 신용정보는 정보주체의 보호와 금융기관의 건전성 제고 양자의 均衡을 유지하는 것이 중요하므로 비공개 정보로 제한하는 것이 타당하다.

---

35) 신용정보법의 개정논의와 관련하여 신용정보의 개념을 再定義(redefinition)해야 한다는 주장이 있다. 정성구, "신용정보법상의 개인정보보호의 문제와 그 개선방향", 한국상사법학회 춘계학술대회 자료집, 2006.5.19, 72면. 그러나 국제적으로 원활한 정보유통을 위해서는 개인정보에 관한 글로벌 스탠더드를 벗어나서는 안될 것이다.

36) 우리나라에서도 금융기관 연체정보(negative information)가 이에 해당한다. 연체정보는 신용정보주체로부터 수집하는 것이 아니라 금융거래 과정에서 금융기관에 자동적으로 축적되는 정보(신용정보법시행령 제2조 1항 3호)이므로 신용정보법에서는 사전 서면동의를 받아야 하는 개인신용정보의 범위에 포함시키지 않고 있다(신용정보법 제23조 1항 4호, 동 시행령 제12조 2항). 이에 대하여 신용정보법 제23조 및 제24조에서 개인의 신용도를 판단하는 데 가장 중요한 연체정보를 제외한 것은 '입법상의 오류'라고 지적하는 견해가 있다. 유니스 김·김성은, "신용정보법 제23조 및 제24조의 개선방향에 대하여", BFL 제16호, 서울대학교 금융법센터, 2006.3, 98면.

다음으로 신용정보의 수집 및 이용, 제3자 제공에 있어서 정보주체의 동의를 어느 수준까지 요구할 것인가 하는 문제가 제기된다. 미국 GLBA와 같이 관련기업 간에 정보를 공유하게 하는 것은 해당 금융기관이나 신용정보회사에는 단연코 유리하지만 정보주체로서는 예측하지 못한 손해나 불편(harm and inconvenience)을 겪게 될 수도 있기 때문이다. 반대로 금융기관이 신용정보를 활용할 때 사전 서면동의를 받아야 한다면 금융기관으로서는 고객과의 거래관계 개설 시 정보의 제공 및 활용이 예상되는 모든 경우를 열거하여 사전동의를 받고자 할 것이다. 이렇게 동의를 받더라도 정보를 제공받는 제3자의 범위나 정보의 활용 목적에 변경이 있는 경우에는 기존 고객들로부터 새로 동의를 받아야 하는데 실무적으로는 거의 불가능에 가까운 일이다. 그렇다고 처음부터 고객으로부터 동의서를 받을 때 포괄동의를 받게 하면 신용정보법의 취지가 목각되고 고객으로서도 자신의 신용정보 사용에 대한 사후 감시 및 통제권을 가질 수 없는 문제가 발생한다.[37]

그렇다고 현행 신용정보법의 규정과 같이 정보주체의 '同意(consent)'를 절대시하고,[38] 동의를 받지 않는 경우에 신용정보법 제23조 및 24조 위반 시의 罰則(유기징역 또는 벌금형)을 적용하는 것은 문제가 있다고 본다. 그 입법취지가 개인신용정보의 目的外 이용, 제3자 제공 시에 개인정보의 자기결정권(self-determinism)을 존중하여 정보주체의 동의를 얻게 하는 것이므로 정보보호의 안전조치(safeguards)를 취하여 개인정보가 침해받을 가능성이 희박하고 오로지 정보주체의 이익을 위하여 활용하는 경우에는 본인의 동의를 받지 않아도 될 것이다(정통망법 제24조 1항 참조). EU지침에서도 개인정보보호의 안전조치가 확보되어 있는 경우에는 정보주체의 동의 요건이 완화되고 있음을 알 수 있다.

신용정보의 적절한 활용은 금융기관의 건전성 유지, 정보주체의 금융이용 가능성 증대를 위하여 중요한 문제이므로 신용정보가 본인의 이익에 반하여 오·남용되지 않도록 안전조치가 확보되어 있는 경우에는 동의 제도를 탄력적으로 운용할 필요가 있다. 우리나라에서도 금융기관의 자산건전성 유지, 信用不良者의 금융소외현상 해소를 위하여 현행 신용정보법의 '본인 동의' 요건을 다소 융통성 있게 운용할 여지는 없는지 검토할 필요가 있다.[39]

---

37) 유니스 김·김성은, 상게 논문, 99면.

38) 신용정보제공동의서가 개인 고객에 대하여 동의서 양식에 포함되어 있는 정보가 향후 개인의신용도를 판단함에 있어서 활용될 것이라는 점에 대한 事前告知로서의 의미를 더 가진다고 생각할 수도 있다. 상게 논문, 99면.

EU지침의 예를 보더라도 例外 사유가 많은 정보주체의 '동의'는 절대적인 것이 아니며 본인에게 이익이 되는 경우에는 개인정보보호를 위한 안전조치가 작동하고 있다는 전제 하에 그 기준을 완화하여도 좋을 것이다. 예컨대, 신용정보제공·이용자가 신용정보보호 안전조치를 취하고 본인의 이익을 위하여 이를 활용하는 경우에는 묵시적인 동의가 있다고 볼 수 있다. 따라서 정보주체에게 이익이 되거나 정보보호의 안전조치가 갖춰진 경우에는 정보주체가 사전·사후에 오프트-아웃 권리를 행사할 수 있게 하고, 그밖의 경우에는 정보주체가 원하는 경우에만 오프트-인 할 수 있게 하는 것이 바람직하다고 생각한다.[40] 미국에서는 EPIC과 같은 시민단체의 노력으로 소비자의 신용정보 보호에 있어 오프트-인을 원칙으로 해야 한다는 주장이 힘을 얻고 있으나 그에 따른 금융기관의 추가비용부담과 금융거래 수수료 인상 가능성에도 주의를 기울여야 할 것이다.[41]

이러한 견지에서 신용정보의 제공 및 활용에 대한 동의를 포지티브 정보에 한하여 정보주체로부터 서면 또는 공인전자문서에 의해서만 동의를 얻도록 한 것은 문제가 있다. 오늘날의 정보화시대에는 그 매체를 제한할 필요는 없으며, 추후 분쟁이 생겼을 때에 대비하여 사실관계를 입증할 수 있도록 본인임을 확인한 녹음, ARS, 전자메시지 기타 요건을 갖춘 방법은 허용하여도 좋을 것이다.

그리고 본인에게 불리한 내용을 포함한 네가티브 정보는 동의의 대상이 아니면서 널리 활용되고 있는 실정이므로 본인이 이를 열람하고 부정확한 정보는 수정·삭제를 요구할 수 있게 하는 등의 방법으로 이를 제도화할 필요가 있다고 본다. 이러한 견지에서 정부가 2006년 4월 신용정보법 시행령 개정안을 마련하면서 신용정보업자 등(예컨대 크레딧 뷰로와 같은 개인신용정보회사)은 인터넷 홈페이지를 통해 신용정보주체가 최근 1년간 그 신용정보주체의

39) 정성구 변호사는 각 개인이 의사결정을 위한 사전정보를 충분히 숙지한 상태에서 동의의 내용을 결정(informed decision)하고 그 형식을 서면으로 하는 것이 바람직하다고 한다. 정성구, 전게 자료집, 72~73면.

40) 이와 같이 신용정보의 내용에 따라 구별하는 게 아니라, 처음부터 고객에게 일정한 경우의 정보공유에 대하여는 사후거부권을 부여하는 것(opt-out)이 형식적인 사전동의를 받게 하는 현행 방식보다 효율적인 개인정보보호방안이라고 주장하는 견해가 있다. 오프트-아웃 권리를 실효성 있게 보장하기 위하여는 고객에 따라 오프트-아웃할 수 있는 정보의 범위를 달리 할 수 있도록 하는 것이 바람직할 것인데 이를 위하여는 고객정보를 세부적으로 관리할 수 있는 전산시스템의 개발이 병행할 필요가 있다고 본다. 상게 논문, 99면.

41) 이에 관하여 실증적 분석을 한 논문으로는 Michael E. Staten & Fred H. Cate, "The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Study of MBNA", 52 Duke L.J. 745 (Feb. 2003) 참조.

신용정보 제공내역을 조회할 수 있도록 하고, 이 경우 신용정보업자등은 금융감독위원회가 정하는 일정 기간(예컨대 6개월)마다 1회 이상 무료로 조회할 수 있도록 한 것은[42] 진일보한 규정이라 생각된다.

이러한 견지에서 미국 GLBA와 같이 비공개 개인정보를 관련이 없는 제3자(unaffiliated third party)에게 제공할 때 오프트-아웃 권리를 부여하는 것만으로는 곤란하다. 정보주체에게 이익이 되는지, 정보보호의 안전조치가 갖춰져 있는지 판단하여 별 문제가 없는 경우에만 오프트-아웃 할 수 있게 하고, 그밖의 경우에는 정보주체가 오프트-인하는 형식으로 동의를 얻어야 할 것이다. 우리나라의 신용정보법은 미국의 GLBA와 입법연혁이나 취지가 다르므로 신용정보제공·이용자의 상호관련성 유무를 기준으로 동의 여부를 의제할 수는 없으며 위와 같은 기준에 입각하여 판단하는 것이 옳다고 생각한다. 그동안 국내 금융기관들은 여러 차례 신용정보법의 개정과 은행연합회의 신용정보관리규약 개정에 따라 개인신용정보의 제공·활용에 대한 동의서 양식을 변경해 왔다. 최근에는 금융감독원이 개인신용정보 관리·보호의 모범규준(Best Practice)을 제정·권고함에 따라[43] 금융감독원의 권고양식을 따르고 있다.

---

42) 재정경제부, "신용평가업 진입규제 완화 등 신용정보인프라 개선(신용정보법 시행령 개정안 입법예고)", 보도자료 2006.3.17자. <http://www.mofe.go.kr/>

43) 금융감독원은 2005년 11월 「개인신용정보 관리·보호 모범규준」을 제시하고 금융회사들이 관련내규 정비와 전산시스템 개발을 마침에 따라 2006년 5월부터 시행에 들어갔다. 금융감독원 2006.5.2 보도자료.
[주요 내용] 금융회사가 여신거래, 카드발급 시에 고객으로부터 징구하는 "개인신용정보 제공·활용 동의서"를 개정하여 고객이 동의내용, 이용목적, 정보활용 및 제공범위 등을 쉽게 이해할 수 있도록 구체적으로 기술하였으며, 금융회사는 고객의 각종 권리사항*을 고객이 충분히 인지할 수 있게 금융회사 인터넷 홈페이지에 동 내용을 상시 게시하고 '고객권리 안내문'을 별지로 작성하여 고객에게 교부하도록 하였다.
[동의철회권의 명시] 고객이 정보내용을 동의한 이후라도 본인의 정보를 제휴회사 등에 제공하는 것을 중단토록 요청(동의철회권)하거나 더 이상 본인에게 성가신 전화 마케팅을 하지 못하도록 요청(Do-Not-Call)하는 경우 금융회사는 이에 응하여야 한다. 이러한 동의철회권, 전화수신거부권 등의 법적 근거를 마련하기 위하여 신용정보법 개정도 추진하기로 했다. 또한, 금융회사는 고객정보를 제공받아 활용하는 제휴회사 등의 정보 오·남용 사례가 없도록 제휴회사 등과 고객정보 보호를 위한 보안관리 약정을 별도 체결하게 된다.
[무료 신용조회서비스 제공] 금융회사 거래고객은 개인신용정보회사(Credit Bureau)의 인터넷 홈페이지를 통하여 무료로 본인 신용정보와 신용등급을 확인(예: 연 1회 1주일간)할 수 있도록 했다. 아울러 금융회사 등은 내부통제 강화를 위하여 준법감시인(監事)의 감독을 받아 종합적이고 체계적인 신용정보 관리와 보호를 전담하는 "신용정보관리·보호인"을 지정·운용하고, 금번 모범규준을 바탕으로 자체적으로 운용할 개인신용정보 관리·보호지침을 마련하여야 한다.

3. 신용정보법의 개정방향

오늘날 피싱, 프리텍스팅, 해킹 기타의 방법으로 신용정보가 한 번 침해되면 그 피해는 예측할 수 없을 정도이다. 그러므로 이에 관한 지식이나 정보가 크게 부족한 개인보다는 정확한 신용정보의 유지·관리가 절대적으로 중요한 금융기관이 정보보안(data security)에 대하여 일차적으로 책임을 지게 할 필요가 있다. 만일 개인이 자신의 신용정보가 침해받았다고 금융기관에 신고한다면 금융기관은 침해 여부를 주의깊게 조사할 의무가 있다.[44]

그리고 미국의 GLBA와 같이 잘못된 신용기록으로 피해를 입지 않도록 신용주체에 대하여 6개월 정도 무료로 간략한 신용조사보고서를 받아보도록 하여야 할 것이다. 금융기관이 직원의 과오나 실수로 고객들의 개인정보를 유출하고도 당장 그 피해 유무를 알 수 없는 개인이 피해를 입은 다음에야 개별적으로 손해배상을 청구하게 하는 식으로는 신용정보가 제대로 보호된다고 할 수 없기 때문이다.

이와 아울러 최근 새로 제정된 「전자금융거래법」[45]의 규정에 의하여 금융기관이 신용정보가 침해되지 않도록 기술적으로나 관리상으로 안전조치를 취해야 할 것이다. 우리나라와 같이 외환금융위기를 경험한 나라에서는 국민의 기

---

44) 2004년 연방고등법원의 판결은 금융기관의 조사의무에 대한 중요한 先例를 확립하였다. 그 계기가 된 사건은 다음과 같다. 미국의 MBNA America Bank (MBNA)가 그의 신용카드 회원인 존슨에게 카드 대금을 청구하면서 파산을 한 그녀 前남편의 카드대금까지 함께 청구하였다. 이에 존슨은 신용정보회사의 자신에 대한 신용조사에 문제가 있다고 보고 이의를 신청하였으며, 이들 신용정보회사는 MBNA에 소비자의 이의에 대한 해명(Automated Consumer Dispute Verification: ACDV)을 요청하였다. 이에 MBNA는 자체 고객정보시스템(Customer Information System: CIS)에 기록되어 있는 자료만 보고 존슨의 신용기록이 정확하다고 ACDV 회신을 하였다. 이에 존슨은 MBNA가 신용보고법(FCRA)에서 요구하고 있는 '합리적인 조사(reasonable investigation)' 의무를 다하지 않았다고 손해배상을 청구하였으며 1심 배심원들은 MBNA가 원고에게 잘못 청구한 금액과 변호사비용 9만여불을 배상하도록 명하였다. MBNA는 은행의 조사의무는 기록을 대조하는 것으로 충분하다고 하였으나 항소심인 제4지구 고등법원에서는 조사란 "채권은행으로서 어느 정도 주의깊은 조사(some degree of careful inquiry)를 요하는 것"이라 하여 1심판결을 받아들였다. *Johnson v. MBNA America Bank NA et al.*, 4th Cir. Case No. 03-1235, February 11, 2004.

45) 전자금융거래법 제8조 2항 2호는 "접근매체의 위조나 변조로 발생한 사고에 대하여 금융기관 또는 전자금융업자가 사고의 방지를 위한 보안절차의 수립과 이의 철저한 준수 등 합리적으로 요구되는 수준의 충분한 주의의무를 다하였음을 입증하는 경우" 그 책임을 면하게 하고 있다. 이 법안은 2006년 4월 6일 국회 본회의에서 통과되어 같은 달 27일 공포되었으며 2007년 1월 1일부터 시행될 예정이다.

본권으로서 개인신용정보의 보호도 중요하지만 그 못지 않게 憲法上의 '公共福利', '幸福追求權' 개념을 원용하여 금융시스템의 안정, 신용불량자의 금융소외 방지 등을 위한 개인신용정보의 제공(onward transfer) 및 활용(processing)을 인정할 필요가 있다고 생각한다. 더욱이 이와 관련된 IT산업의 발전을 도모하기 위해서는 민간의 자율성을 확대하고 기술적인 해결방법(solution)을 인정하는 것이 더욱 긴요시된다고 하겠다.

구체적으로 신용정보법 관련규정의 개정방향에 대하여 논의하자면 일반적인 신용정보는 여전히 높은 수준의 동의(opt-in)를 요하지만, 동법 시행령 제2조에서 정하는 신용거래정보(제2호)와 거래능력정보(제4호)는 낮은 수준의 동의(opt-out)만 있어도 족한 것으로 하여 정보의 유통 및 가공처리가 이루어질 수 있도록 해야 할 것이다. 요컨대 신용정보법 제23조(개인신용정보의 제공·활용에 대한 동의) 제1항 제4호 및 시행령 제12조 제2항의 규정은 낮은 수준의 동의만 얻어도 되게끔 개정할 필요가 있다고 생각한다.

이상의 논의에 입각하여 신용정보법 중 정보주체의 동의에 관한 개정시안을 만들어보면 <별표>와 같다. 2004년과 2005년에 걸쳐 순차로 국회에 제출된 노회찬 의원, 이은영 의원, 이혜훈 의원의 「개인정보보호기본법(안)」에 의하면 민간부문과 공공부문으로 나뉘어 있는 개인정보보호를 통합할 것인지, 아니면 현행과 같이 유지할 것인지에 관하여는 서로 입장을 달리하고 있으나, 신용정보법은 현행대로 두는 것을 전제로 하고 있다.[46]

46) 각각의 법안에 대하여는 국회 홈페이지<http://www.assembly.go.kr>의 의안정보 시스템에서 그 내용을 살펴볼 수 있다.

〔별표〕 신용정보의 이용 및 보호에 관한 법률 및 동 시행령의 개정시안

- 신용정보의 제공·활용에 대한 동의제도의 개선을 중심으로 -

(밑줄친 부분이 새로 신설되는 조항임)

구 분	개정 시안 조문
법 률	제23조(개인신용정보의 제공·활용에 대한 동의) ① 신용정보제공·이용자는 다음 각호에서 정하는 개인에 관한 신용정보(이하 "개인신용정보"라 한다)를 신용정보업자등에게 제공하고자 하는 경우에는 대통령령이 정하는 바에 의하여 당해 개인으로부터 서면 또는 공인전자서명(전자서명법 제2조제3호의 공인전자서명을 말한다. 이하 같다)이 있는 전자문서(전자거래기본법 제2조제1호의 전자문서를 말한다. 이하 같다)에 의한 동의를 얻어야 한다. 다만, 신용정보제공·이용자가 자체적으로 수집한 정보 또는 개인신용정보를 그의 사용목적을 위하여 가공처리한 정보는 그러하지 아니하다. 1. 금융실명거래 및 비밀보장에 관한 법률 제4조의 규정에 의한 금융거래의 내용에 관한 정보 또는 자료 2. 개인의 질병에 관한 정보 3. 개인의 성명·주소·주민등록번호(외국인의 경우 외국인등록번호 또는 여권번호)·성별·국적 및 직업 등 개인을 식별할 수 있는 정보 4. 기타 대통령령이 정하는 개인신용정보 ② 제1항의 규정에 불구하고 신용정보제공·이용자가 개인신용정보 중 제1항제3호에 해당하는 정보를 제공하고자 하는 경우에는 전화에 의한 본인의 동의나 인터넷 홈페이지의 동의란에 본인 이행하는 동의표시에 의하여 신용정보업자등에게 제공할 수 있다. ③ 제1항의 규정에 불구하고 제1항제4호에 해당하는 정보로서 본인이 녹음, 자동응답시스템(ARS), 전자메시지(SMS) 기타 본인임을 확인할 수 있는 방법에 의하여 본인임을 확인하고 이에 동의한 정보는 제1항의 동의를 한 것으로 본다. 신용정보제공·이용자가 제1항제4호에 해당하는 개인신용정보를 그의 보호를 위한 안전조치를 취하고 오로지 신용정보주체의 이익을 위하여 활용하는 경우에는 당해 신용정보주체가 그 정보제공 및 활용에 동의한 것으로 본다. 그러나, 신용정보주체는 언제든지 그의 동의를 철회할 수 있다. ④ 신용정보주체가 자신의 개인신용정보가 침해받았다고 신용정보제공·이용자에게 신고한 때에는 신용정보제공·이용자는 지체없이 그 침해여부를 조사하고 대통령령이 정하는 조치를 취하여야 한다.

시행령	제12조 (개인신용정보의 제공·활용에 대한 동의등) ① 법 제23조의 규정에 의하여 당해 개인으로부터 서면 또는 공인전자서명(전자서명법 제2조제3호의 규정에 의한 공인전자서명을 말한다)이 있는 전자문서(전자거래기본법 제2조제1호의 규정에 의한 전자문서를 말한다)에 의한 동의를 얻고자 하는 경우에는 금융감독위원회가 정하는 바에 의하여 제공할 신용정보의 내용, 제공대상자등을 명기한 동의서에 의하여야 한다. ② 법 제23조제1항제4호에서 "기타 대통령령이 정하는 개인신용정보"라 함은 제2조제1항제2호 및 제4호의 정보 중에서 개인에 관한 정보를 말한다. ③ 법 제23조제4항에서 "대통령령이 정하는 조치"라 함은 개인신용정보가 침해받았다고 신고한 신용정보주체에 대하여 6개월간 신용정보제공·이용자의 비용으로 본인의 신용등급변동 여부를 확인할 수 있는 신용조사보고서를 제공하는 것을 말한다.

참고: 신용정보법 및 동 시행령상 신용정보의 정의

[신용정보법] 제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "신용정보"라 함은 금융거래등 상거래에 있어서 거래상대방에 대한 식별·신용도·신용거래능력등의 판단을 위하여 필요로 하는 정보로서 대통령령 이 정하는 정보를 말한다.
   <후략>

[신용정보법 시행령] 제2조 (정의)

① 법 제2조제1호에서 "대통령령이 정하는 정보"라 함은 다음 각호의 1에 해당하는 정보를 말한다. 다만, 법 제2조제8호·제9호 및 제11호의 업무와 관련하여서는 다른 법령의 규정에 의하여 공시 또는 공개되거나 다른 법령에 위반됨이 없이 출판물·방송 등의 공공매체 등을 통하여 공시 또는 공개된 정보 등은 제외한다.
   1. 개인의 성명·주소·주민등록번호(외국인의 경우 외국인등록번호 또는 여권번호)·성별·국적 및 직업 등과 기업 및 법인의 상호·법인등록번호·사업자등록번호·본점 및 영업소의 소재지·설립연월일·목적 및 임원에 관한 사항 등 특정 신용정보주체를 식별할 수 있는 정보(제2호

내지 제6호의 1에 해당하는 정보와 결합되는 경우에 한한다)

2. 대출·보증·담보제공·가계당좌예금 또는 당좌예금·신용카드·할부금융·시설대여 등의 금융거래 등 상거래와 관련하여 신용정보주체의 거래내용을 판단할 수 있는 정보로서 재정경제부령이 정하는 정보
3. 금융거래 등 상거래와 관련하여 발생한 연체·부도·대지급 또는 허위 기타 부정한 방법에 의한 신용질서 문란행위 등 신용정보주체(신용정보 주체가 회사인 경우에는 다음 각목의 자를 포함한다)의 신용도를 판단할 수 있는 정보로서 재정경제부령이 정하는 정보
   가~라. 생략
4. 금융거래 등 상거래에 있어서 신용도 등의 판단을 위하여 필요한 개인의 재산·채무·소득의 총액, 납세실적 등과 기업 및 법인의 연혁·주식 또는 지분보유현황 등 회사의 개황, 판매내역·수주실적·경영상의 주요 계약 등 사업의 내용, 재무제표 등 재무에 관한 사항, 주식회사의 외부감사에 관한 법률의 규정에 의한 감사인의 감사의견 및 납세실적 등 신용정보주체의 신용거래능력을 판단할 수 있는 정보
5. 금융거래 등 상거래에 있어서 신용정보주체의 식별·신용도 및 신용거래능력을 판단할 수 있는 법원의 심판·결정정보, 조세 또는 공공요금 등의 체납정보, 주민등록 및 법인등록에 관한 정보 및 기타 공공기관이 보유하는 정보로서 재정경제부령이 정하는 정보
6. 제2호 내지 제5호와 유사한 신용정보로서 재정경제부령이 정하는 정보

참고 문헌

유니스 김·김성은, “신용정보법 제23조 및 제24조의 개선방향에 대하여”, BFL 제16호, 서울대학교 금융법센터, 2006.3.

박훤일, “개인정보의 보호를 위한 안전조치 - 개인정보보호 기업규칙(BCRs)을 중심으로”, 「경희법학」 제40권 2호, 2005.12.30.

_____, 「EU 개인정보보호지침 준상호주의 이행방안 연구」, 한국정보보호진흥원 최종연구보고서: 개인정보연구01-02, 2001.11.

부기덕, “금융가산책: 개인정보보호법 제정과 금융기관의 대응”, 「대은 경제리뷰」, 대구은행, 2005.

정성구, “신용정보법상의 개인정보보호의 문제와 그 개선방향”, 한국상사법학회 춘계 학술대회 자료집, 2006.5.19.

재정경제부, “신용평가업 진입규제 완화 등 신용정보인프라 개선(신용정보법 시행령 개정안 입법예고)”, 보도자료 2006.3.17자.

Andrew J. Morris, Brian W. Smith, Kimberly Kiefer and Cregory S. Feder, "4.06 Financial Institutions: Agency and Industry Initiatives", *E-Commerce Financial Products And Services*, ALM Properties, Inc., 2005.

Michael E. Staten and Fred H. Cate, "The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Study of MBNA", 52 Duke L.J. 745 (Feb. 2003).

Electronic Privacy Information Center (EPIC), "The Gramm-Leach-Bliley Act," January 2005. <http://www.epic.org/privacy/glba/>

Sun Microsytems, *Privacy and Data Protection: Mitigating the Risks of Information Exposure, A Technical White Paper,* July 2004.

재정경제부 홈페이지 <http://www.mofe.go.kr/>

금융감독원 홈페이지 <http://www.fss.or.kr/kor/koreanIndex.htm>

미국 하원 금융서비스위원회 홈페이지 <http://financialservices.house.gov/>

[이상 웹사이트 2006.7.1 최종 접속]

Protection of Personal Credit Information in the Cross-border Financial Transactions

Park, Whon-Il*

These days consumers are increasingly concerned about any possible chance of abuse and misuse of their credit information. Upon hearing endless reports of numerous ID theft and leakage of personal information, the affected data subjects are inclined to file lawsuits for compensation in group against such game companies and financial institutions as deemed responsible for the incidents.

However, in the Information Age, it is useless and unwise to hide personal information. Brisk flow of favorable credit information will enhance considerably credit availability and job opportunities of a data subject. For example, in the Internet banking, active flow of credit information is conducive to the appropriate risk management of financial institutions. It is also helpful to assess the credit standing and to identify financial needs of customers so as to develop new financial products and to conduct aggressive marketing.

The situation is all the more important in cross-border financial transactions. If an unauthorized use of a person's credit information results in credit fraud in a foreign country, we cannot figure out the scope of financial damage to the data subject as well as irrecoverable damage to his credit.

In this case, we can count the EU Directive on data protection, which regulates the conditional data export to a third country, as a universal norm governing credit data flow. In the United States, there are the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act. In particular, the GLBA purports to supplement the existing privacy provisions of the FCRA.

* Assistant Professor of Law at Kyung Hee University.

The GLBA financial privacy rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and once a year thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the consumer's right to opt-out of the information being shared with unaffiliated parties. On the other hand, the GLBA safeguards rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. This plan must include: ⅰ) denoting at least one employee to manage the safeguards, ⅱ) constructing a thorough risk management on each department handling the nonpublic information, ⅲ) developing, monitoring, and testing a program to secure the information, and ⅳ) changing the safeguards as needed with the changes in how information is collected, stored, and used. In 2003, FCRA was amended by the Fair and Accurate Credit Transactions Act (FACTA, Public Law 108-159) to guard against identity theft.

Once a credit information is infringed upon by means of phishing, pretexting, hacking and other illegal act, the resulting damage is almost immeasurable. So the financial institution is primarily held responsible for the data security of financial information of its customers. If a customer argues that his credit information is hurt by negligent management of financial institutions, they have to investigate disputed information. Also, users of the information for credit, insurance, or employment purposes must notify the consumer when an adverse action is taken on the basis of such reports. A proposed amendment to the GLBA (H.R. 3997) will oblige the relevant financial company to provide free credit report service to the affected customers so that the accuracy and completeness of the report may be verified or contested by them. It sounds reasonable because customers are not in a position to know the occurrence of, or to identify, the real damage arising out of the infringement upon their credit information.

In Korea, the Act concerning the Use and Protection of Credit Information (the "Act") has been under in-depth discussion and year-long debates for the necessary revision. At present, three amendments to the Act have been presented

to the National Assembly by lawmakers of the Ruling Party and the Opposition Parties.

In short, the writer has an opinion that the identity information requires the high-level "opt-in" consent of the data subject, while a low-level negative consent or "opt-out" is necessary for the credit transaction information (Item 2 of Article 2, the Enforcement of Decree of the Act) and the credit capacity information (Item 4 of the said Decree). It is very helpful to the banking industry to promote the data flow and to process such credit information.