개인정보 유출 관련 판례 및 금융권 시사점

금융정보보호부 과장 유정각(kagi@kftc.or.kr)
대리 송주민(jumin@kftc.or.kr)

Ⅰ. 개요 129

Ⅱ. 개인정보 관련 법률 129

Ⅲ. 개인정보 유출 관련 판례 131
1. 엔씨소프트 사건 131
2. A은행 사건 132
3. LG전자 사건 134
4. 옥션 사건 136
5. GS칼텍스 사건 138

Ⅳ. 금융권 시사점 140
1. 개인정보 유출기업의 책임에 대한 이해 140
2. 개인정보 위험관리 방안 마련 145

참고문헌 148

〈요 약〉

지난 2010년 한해동안 약 1억건 이상의 개인정보 침해사고가 발생하는 등 개인정보 침해가 대형화 · 지능화 · 다양화됨에 따라 개인정보보호에 대한 사회적 경각심이 높아지고 있다. 2011년 3월 29일 개인정보보호에 관한 일반법으로 「개인정보보호법」이 공포되고, 개인정보 유출 피해자들이 유출기업을 대상으로 적극적인 손해배상소송을 제기하는 등 개인정보 유출기업의 책임은 갈수록 커지고 있다. 특히, 금융기관은 업무 특성상 고객의 개인정보를 많이 활용하고 있으므로 개인정보를 안전하게 보호하여 고객의 개인정보에 대한 권리와 이익을 보장할 의무가 있으며, 만약 개인정보가 유출된다면 경영진의 불구속 입건 및 손해배상과 같은 민 · 형사상 책임을 비롯한 규제당국의 간섭, 기업 이미지 하락 등 다양한 책임을 지게 될 것으로 보여진다.

이에 본고에서는 엔씨소프트 사건, A은행 사건, LG전자 사건, 옥션 사건, GS칼텍스 사건 등 주요 개인정보 유출 관련 판례를 비교 · 분석함으로써 유출사고 발생시 금융기관의 책임을 이해하고 효과적인 개인정보 위험관리 방안을 마련하고자 한다.

관련 판례를 분석해보면, 개인정보 유출기업의 책임을 정하는 주요 쟁점은 ① 개인정보가 관리 · 통제권을 벗어나 제3자가 알 수 있는 상태에 이르렀는지 ② 유출된 정황이 금전으로 손해배상할 수준인지 ③ 개인정보 유출기업이 주의의무를 위반하였는지 ④ 해당 기업의 손해배상 책임범위가 어느 정도인지 등으로, 단순히 유출사고 발생 당시의 상황 뿐만 아니라 사고 발생 전후의 조치들에 의해서도 영향을 받는다.

따라서 금융기관은 평상시에는 개인정보의 수집, 이용, 제공, 파기 등 단계별로 요구되는 보호기준을 준수하고, 기술적 · 관리적 · 물리적 보호조치를 충분히 이행하는 것은 물론 개인정보 영향평가를 통해 개인정보 유출 위험요인을 분석하여 개선사항을 도출하며 개인정보 유출사고에 대비한 대응 매뉴얼 등을 마련하는 것이 필요하다. 그리고 유출사고 발생시에는 유출정보의 성격, 규모, 확산 범위, 유출로 인한 피해의 정도, 사고당시 취하고 있던 보호조치의 수준, 유출의 원인 등을 파악하고 관련 증거들을 수집해야 한다. 또한 개인정보 유출사실을 지체 없이 피해 고객에게 통지하고, 피해 고객들의 피해현황 접수를 받을 수 있는 창구를 마련하는 것은 물론 신속하고 적절한 피해 확산방지 및 피해회복 조치를 통해 추가적인 피해를 최소화하고 피해 고객들의 권리를 구제하고자 노력해야 한다.

Ⅰ. 개요

개인정보란 생존하는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통해 개인을 알아볼 수 있는 정보를 말하며, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 모두 포함하고 있다.

개인정보 침해는 대형화 · 지능화 · 다양화되고 있으며, 2010년 한해동안 약 1억건 이상의 개인정보 침해사고가 발생하는 등 개인정보보호에 관한 사회적 경각심이 높아지고 있다. 또한 개인정보에 대한 국민의 권익을 보장하고자 제안된「개인정보보호법」이 2011년 3월 공포되었고 개인정보 유출 피해자들이 유출기업을 대상으로 적극적인 손해배상소송을 제기하는 등 개인정보 유출기업의 책임은 갈수록 커지고 있다.

특히 금융기관은 업무 특성상 고객의 개인정보를 많이 활용하고 있으므로, 만약 개인정보가 유출된다면 벌금 · 과태료 부과 및 경영진의 불구속 입건과 같은 형사적 책임, 개인정보 유출 피해자들에 대한 손해배상 책임, 그 외 규제당국의 간섭 및 기업 이미지 하락 등 다양한 책임을 지게 될 것으로 보여진다. 따라서 본고에서는 개인정보 유출 관련 판례를 정리하고 분석함으로써, 개인정보 유출기업의 책임을 명확히 이해하는 것은 물론 유출사고 발생시 책임을 최소화하고 고객의 개인정보를 안전하게 보호할 수 있는 효과적인 개인정보 위험관리 방안을 모색해 보고자 한다.

제II장에서는 현 개인정보 관련 법률 체계와 개인정보보호법 제정으로 인해 달라지는 부분에 관해 간략히 살펴본다. 제III장에서는 엔씨소프트 사건, A은행 사건, LG전자 사건, 옥션 사건, GS칼텍스 사건 등 대표적인 개인정보 유출 관련 판례들에 대해 자세히 정리한다. 마지막으로 제IV장에서는 앞서 살펴본 개인정보 유출 관련 판례를 분석하여 금융권에 시사하는 바와 준비해야 할 사항에 대해 살펴보도록 한다.

Ⅱ. 개인정보 관련 법률

현재 개인정보 관련 법률체계는 금융, 정보통신, 공공, 교육, 의료 등 주요 분야별로 소관 법령이 나누어져 있다(표1 참조). 그런데 이와 같은 체계에서는 법 적용의 사각지대가 존재하고, 개별법간 처리 기준이 상이하여 혼란을 초래하는 경우도 있었다. 또한「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 제외하고 각각의 개별법에서는 개인정보보호 관련 조항이 제한적이거나 선언적인 규정에 그치고 있어, 개인정보보호에 관한 일반법

인 「개인정보보호법」의 필요성이 사회적으로 대두되었다.

이에 2008년 개인정보보호법안이 발의되었고, 2011년 3월 29일 공포되어 9월 30일부터 시행된다.

〈표1〉 개인정보보호법 제정 전 개인정보 관련 법률체계

분야	소관 법령
금융 · 신용	신용정보의 이용 및 보호에 관한 법률
정보통신	정보통신망 이용촉진 및 정보보호 등에 관한 법률
공공 · 행정	공공기관의 개인정보보호에 관한 법률
교육	초 · 중등교육법
의료	생명윤리 및 안전에 관한 법률

개인정보보호법안의 주요내용은 다음과 같다. 우선 개인정보보호법의 적용대상을 공공 · 민간 부문의 모든 개인정보처리자로 확대하고, 전자적으로 처리되는 개인정보 외에 수기문서까지 개인정보의 보호범위에 포함하고 있다. 개인정보의 처리에 있어 수집 · 이용 · 제공 · 파기 등 단계별로 보호기준을 강화하고 있으며, 개인정보의 분실 · 도난 · 유출 · 변조 및 훼손을 방지하기 위하여 기술적 · 관리적 · 물리적 보호조치를 취하도록 의무화하고 있다.

개인정보처리자가 개인정보 유출 사실을 인지하였을 경우 지체없이 해당 정보주체에게 관련사실을 통지하고, 일정 규모 이상의 개인정보가 유출된 때에는 전문기관에 신고하도록 하고 있다. 그리고 정보주체의 권리를 보장하기 위하여 정보주체에게 개인정보의 열람청구권, 정정 · 삭제 청구권, 처리정지 요구권 등을 부여하고 있으며, 개인정보처리자는 정보주체가 열람 등을 요구할 수 있는 구체적인 방법과 절차를 마련하고 이를 공개하도록 규정하고 있다.

또한 개인정보 피해구제제도를 개선하고자 집단분쟁조정제도 및 단체소송제도를 도입하고 있다. 개인정보에 관한 분쟁조정 업무를 신속하고 공정하게 처리하기 위하여 개인정보분쟁조정위원회를 두고, 개인정보 피해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생하는 경우 분쟁조정위원회에 일괄적인 분쟁조정을 의뢰 또는 신청할 수 있다. 개인정보처리자가 분쟁조정위원회의 조정을 거부하거나 조정결과를 수락하지 아니한 경우, 법에서 정한 요건에 해당하는 단체는 법원에 행위의 금지 · 중지를 구하는 단체소송을 제기할 수 있다. 마지막으로 개인정보에 관한 권리 또는 이익을 침해받은 사실을 신고하고 상담할 수 있는 창구를 마련하고자, 개인정보 침해사실의 신고제도를 도입하고 있다.

개인정보보호법은 개인정보보호의 사각지대를 없애고 개인정보 침해로 인한 국민의 피해 구제를 강화하여 개인정보에 대한 권리와 이익을 보장하는 것을 목적으로 하고 있어, 금융권을 비롯한 사회 전반에 많은 영향을 미칠 것으로 예상된다. 개인정보보호법 제정에 따른 금융권의 기술적 · 관리적 · 물리적 세부 조치사항 등은 개인정보보호법 시행령, 시행규칙, 관련 고시 및 지침 등을 통해 구체화될 것으로 예상된다.

Ⅲ. 개인정보 유출 관련 판례

본 장에서는 개인정보 유출 관련 주요 판례에 대해 자세히 살펴보고자 한다(표2 참조).

〈표2〉 개인정보 유출 관련 주요 판례

사건명	사건번호	선고일자 등
엔씨소프트 사건	2006나12182	서울중앙지방법원 2007.1.26 선고
A은행 사건	2007나33059	서울고등법원 2007.11.27 선고
LG전자 사건	2008나25888	서울고등법원 2008.11.25 선고
옥션 사건	2008가합31411	서울중앙지방법원 2010.1.14 선고
GS칼텍스 사건	2008가합90021, 2008가합88370	서울중앙지방법원 2010.9.16 선고

1. 엔씨소프트 사건

가. 사건개요

엔씨소프트는 온라인 게임인 리니지II 게임을 개발하여 그 이용서비스를 제공하는 회사이다. 2005년 5월 11일 엔씨소프트의 담당직원이 리니지II 게임 서버 및 네트워크의 정기점검 작업을 실시하면서 아이디 및 비밀번호 입력과 관련된 기능을 점검하기 위해 키보드로 입력한 아이디 및 비밀번호가 이용자의 컴퓨터 하드디스크에 로그파일로 기록되도록 하였다. 기능 점검 후 실수로 아이디 및 비밀번호 기록기능을 삭제하지 않은 채 정기점검 작업을 마치는 바람에 2005년 5월 11일 오전 10시부터 2005년 5월 16일 12시 20분까지 리니지II 게임에 접속한 이용자들의 아이디와 패스워드가 로그파일에 기록되었다.

엔씨소프트는 사고기간 동안 리니지II 게임서버에 접속했던 모든 이용자들로 하여금 주민등록번호를 통한 동일인 확인을 거쳐 새로운 비밀번호로 변경한 후에만 리니지II 게임에

접속할 수 있도록 하는 비밀번호 강제변경 조치를 취했고, 리니지II 게임 홈페이지에 이용자들에 대한 사과문을 게시하였다.

나. 판결요지

아이디와 비밀번호는 가상공간에서 그 행위자의 인격을 표상한다고 할 수 있으므로, 당해 개인을 알아볼 수 있는 개인에 관한 정보로서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 한다)」 제2조 제1항 제6호에서 정한 개인정보에 해당한다.

원고(피해이용자)들은 자신들의 의사에 반하여 개인정보가 함부로 공개되지 아니할 권리를 가지며, 원고들의 개인정보를 수집 · 관리하는 정보통신서비스 제공자인 엔씨소프트는 원고들의 개인정보가 누출되지 않도록 보안조치를 다하여야 할 주의의무가 있다. 그럼에도 불구하고 엔씨소프트는 리니지II 게임 서버의 정기점검 과정에서 원고들의 개인정보인 아이디 및 비밀번호가 암호화되지 않은 상태로 로그파일에 기록되도록 함으로써 이와 같은 주의의무를 위반하였다.

정보통신망법 상의 누출이라 함은 개인정보가 정보통신서비스 제공자 및 이용자의 개인정보 관리 · 통제권을 벗어나 당해 개인정보를 모르는 제3자가 그 내용을 알수 있는 상태에 이르는 것을 의미한다고 할 수 있다. 따라서 사고기간 동안 PC방 컴퓨터에서 리니지II 게임에 접속하여 PC방 컴퓨터에 로그파일이 저장된 경우는 개인정보 누출로 보고, 집의 개인용 컴퓨터에서 리니지II 게임에 접속하여 개인용 컴퓨터에 로그파일이 저장된 경우는 개인정보 누출로 보지 않는다.

개인정보 누출로 인하여 헌법에 의하여 보장된 원고들의 기본권인 자신들의 의사에 반하여 개인정보가 함부로 공개되지 아니할 권리가 침해되었는 바, 원고들이 이 사건 사고로 받은 정신적 고통은 통상손해로 볼 수 있다. 따라서 엔씨소프트는 원고들에게 위자료를 지급할 의무가 있으며, 위자료는 각 10만원을 인정한다.

2. A은행 사건

가. 사건개요

2006년 3월 15일 A은행 직원이 복권서비스 이용계약을 체결한 가입회원들에게 서비스 안내 이메일을 발송하는 과정에서 회원 32,377명의 성명, 주민등록번호, 이메일 주소 등

이 수록된 텍스트 파일을 이메일 첨부파일로 전송하는 사고가 발생하였다. A은행 직원은 이메일 전송 후 회원정보가 이메일에 첨부된 사실을 알고, 이메일 전송을 강제중단하였으나 이미 3,723명의 회원들에게 이메일 발송이 완료되었다.

사건 발생 후 A은행은 이메일이 발송된 회원 3,723명의 이메일 계정을 관리하는 포털사이트에 요청하여 이미 열람한 641명을 제외한 나머지 회원들에게 전송된 이메일을 회수하고, 이미 열람한 회원들에게는 이메일을 삭제하여 줄 것을 요청하였다. 또한 A은행 웹 사이트 내에 고객정보유출 피해접수센터를 개설하여 고객정보 유출 여부 조회 및 피해접수 창구를 마련하는 한편, 회원 32,377명에게 정보도용 차단서비스를 1년간 무료로 이용할 수 있는 서비스를 제공하였다.

나. 판결요지

A은행은 원고(피해고객)들의 개인정보가 누출되지 않도록 필요한 관리적 조치를 다하여야 할 주의의무가 있음에도 불구하고, 이메일을 전송하는 과정에서 원고들의 개인정보를 첨부파일로 전송하여 이메일을 수신한 자들이 개인정보를 취득할 수 있게 함으로써 주의의무를 위반하였다 할 수 있다. 개인정보 누출로 인하여 헌법에 의하여 보장된 원고들의 기본권인 자신들의 의사에 반하여 개인정보가 함부로 공개되지 아니할 권리가 침해되었는바, 원고들이 이 사건 사고로 받은 정신적 고통은 통상손해로 볼 수 있다. 따라서 A은행은 원고들에게 위자료를 지급할 의무가 있다.

손해배상책임의 범위는 쌍방의 참작사유를 함께 고려하여 성명, 주민등록번호, 이메일 주소의 정보가 누출된 원고들에게는 각 20만원, 성명과 이메일 주소가 누출된 원고들에게는 각 10만원의 위자료를 인정한다.

손해배상책임의 범위를 정함에 있어, A은행 참작사유는 아래와 같다.

① 이메일 발송대상 회원 중 약 1/10 정도에게만 이메일이 발송된 상태에서 발송을 중단하고 이메일을 회수하는 등 사후조치를 신속하게 취함에 따라 개인정보가 유포되는 범위를 줄임으로써 그 악용 또는 도용 가능성을 감소시킨 점
② 누출된 개인정보가 실제로 악용 또는 도용되었다는 사실이 밝혀지지 않은 점
③ 누출된 개인정보는 개인의 이메일 계정으로 전송되어, 이메일을 받은 사람 외에 일반인의 접근이 가능한 상태에까지 이르지 않은 점
④ 이 사건 사고는 A은행 직원의 단순 실수로 인한 것으로서, A은행이 영업상 이익을 추구하는 과정에서 개인정보보호시스템에 중대한 하자를 야기하였거나 이를 방치하여 개인정보보호를 태만히 한 것으로 보이지 않는 점 등

손해배상책임의 범위를 정함에 있어, 원고측 참작사유는 아래와 같다.

① 누출된 개인정보인 성명, 이메일 주소, 특히 주민등록번호는 원고들 개개인에 대한 식별수단으로서 그 유출로 인하여 신분도용의 문제까지 발생할 수 있는 중요정보인 점
② A은행은 이들 정보를 담은 파일에 대한 암호화조치를 제대로 하지 않아 유출된 파일을 받은 사람이 이를 손쉽게 열어볼 수 있었고, 더군다나 이들 정보는 서로 결합됨으로써 개인 식별 가능성이 훨씬 커지는데 이 사건에서는 위 정보들이 '성명, 주민등록번호, 이메일 주소' 또는 '성명, 이메일 주소'의 형태로 서로 결합되어 유출된 점
③ 개인정보는 상품이나 서비스를 제공하는 사업자에게는 홍보활동 등의 유용한 영업수단이 되는 바, 이를 영리적으로 이용하는 사업자로서는 그에 따른 모든 책임도 부담하여야 할 것인 점
④ A은행은 원고들이 복권서비스 가입시 고객이 제공한 개인정보를 소중히 여기며 그 보호에 최선을 다할 것을 다짐한다는 등의 「개인정보보호방침」을 인터넷에 게시하였을 뿐 아니라, 가입자들로부터 개별 동의를 받는 「전자금융기본거래약관」 제24조에도 A은행의 관리 소홀로 인한 정보 유출시에는 A은행이 책임을 진다고 규정하는 등 스스로 개인정보보호의 책임을 다할 것을 다짐하여 서비스 가입자들을 안심시켰던 점 등

3. LG전자 사건

가. 사건개요

LG전자는 2006년 9월 3일 2006년도 하반기 신입사원 채용공고를 하고, 2006년 9월 4일부터 2006년 9월 19일까지 LG전자 채용사이트를 통하여 인터넷으로 신입사원 지원을 받았는데, LG전자 입사지원자들은 이 채용사이트에서 입사지원서를 작성하였다. LG전자 서류전형에서 불합격통지를 받은 이 중 한명이 2006년 9월 26일 22시 30분경 다음 포털사이트의 취업정보 공유카페 게시판에 'LG전자의 모든 지원서는 누구나 볼 수 있다'라는 제목으로 입사지원서를 볼 수 있는 링크파일을 첨부하여 게시하였다. 2006년 9월 26일 23시 25분경까지 이 글의 조회수는 3,056회에 달하였다. 위 링크파일을 실행하면 입사지원자들의 사진이 나타나고, 사진을 클릭하면 기본인적사항(성명, 주민등록번호 등), 상세인적사항(학력, 학점 등), 자기소개, 경력, 연구실적 등의 하부메뉴가 있는 페이지가 나타난다.

LG전자는 2006년 9월 27일 0시 8분경 입사지원자들의 등록정보 열람이 불가능하도록 채용사이트 서버의 접속을 차단하였고, 같은날 19시 40분경 LG전자 홈페이지에 공식 사과문을 게재하였다. 전산자료를 통해 확인한 결과, 위 링크파일을 실행하여 비정상적 방법으로 입사지원자들의 등록정보를 열람한 IP주소는 671개였고, 3천여명의 입사지원서가 열람당하였다.

나. 판결요지

「공공기관의 개인정보보호에 관한 법률」에 의하면 공공기관 외의 개인 또는 단체는 컴퓨터를 사용하여 개인정보를 처리함에 있어 공공기관의 예에 준하여 개인정보 보호조치를 강구하도록 규정하고 있으므로, LG전자는 입사지원자들이 자신의 개인정보를 제공한 목적에 반하여 유출되거나 훼손되지 않도록 당시의 기술수준에 부합하는 보안조치를 취하여야 할 주의의무가 있다.

LG전자 입사지원사이트의 웹서버에 웹 방화벽을 적용하지 않고 있었던 점, 입사지원자의 지원서 내용을 열람할 수 있는 URL 중 특정 변수의 인자값을 변경하여 입력하면 위 사이트에 침입하여 타인의 입사지원서를 열람할 수 있는 보안취약점을 간과한 점, 같은 방법으로 다른 대기업의 입사지원사이트에도 침입을 시도하였으나 LG전자 등 4개 회사를 제외하고는 보안장치에 막혀 그 뜻을 이루지 못한 점 등에 비추어보면, LG전자는 당시의 기술수준에 비추어 보더라도 신입사원의 채용을 위한 목적으로 보관중인 개인정보의 분실 · 도난 · 누출 등 방지에 필요한 보안조치를 취하여야 할 주의의무를 위반하였다 할 수 있다.

LG전자의 손해배상책임의 범위를 통상적인 개인정보 침해사건에 비하여 무겁게 볼 사유와 가볍게 하는 사유를 모두 고려하면, 위자료의 액수는 각 30만원으로 정함이 상당하다. 단, 입사지원을 위한 등록정보를 열람당한 경우에만 위자료 청구를 인정하고, 단순히 열람당할 가능성이 있었다는 점만으로는 위자료 청구를 인정하지 않는다.

손해배상책임의 범위를 정함에 있어, 통상적인 개인정보 침해사건에 비하여 무겁게 보는 사유는 아래와 같다.

① LG전자의 보안조치는 당시의 기술수준에 비추어 충분하다고 볼 수 없는 점
② LG전자 시스템의 모니터링이 아니라 다른 인터넷 게시판의 모니터링을 통하여 이 사건 사고를 발견하였고, 그로부터 1시간 8분이 경과한 후 해당 웹 서버가 차단되기까지 입사지원자들의 정보를 열람할 수 있었던 점

③ 사고 발생 하루 후에 입사지원사이트에 사고발생사실을 게시하였을 뿐 입사지원자들에게 이메일 등을 통해 안내한 바 없고, 소송에 이르기 전까지 입사지원자들에게 개인정보 유출 여부와 유출된 정보가 무엇인지 확인하여 준 바 없는 점
④ 개인사, 가족관계, 가치관 등 사적인 영역의 민감한 정보까지 침범당하였던 점
⑤ 위 게시글이 3,056회의 조회수를 기록하였고, 입사지원자들의 등록정보를 열람한 IP주소가 671개이며, 3천여명의 입사지원서가 열람당한 점

손해배상책임의 범위를 정함에 있어, 통상적인 개인정보 침해사건에 비하여 가볍게 하는 사유는 아래와 같다.

① LG전자는 성명, 주민등록번호 등 기본적 인적사항은 별도로 보관하고 Master ID에 의하여만 접근할 수 있도록 하는 등 나름대로 보안조치를 취하였던 점
② 사고 발생 후 해킹방지시스템을 보완하는 등의 조치를 취한 점
③ 미흡하나마 입사지원사이트에 사고발생사실을 알리고 사과 및 재발방지를 다짐한 점
④ 성명, 주민등록번호 등은 열람된 바 없고, 유출된 정보에 의하더라도 지인이나 주변 사람이 아니면 실제 신원을 구체적으로 특정하기는 어려웠을 것으로 보이는 점
⑤ 저장이나 재전송 등이 어려운 방식으로 열람되었고, 유출된 정보의 경제적 가치에 비추어 2차적인 피해 확산 가능성은 높지 아니한 점
⑥ 누출된 개인정보가 추가로 외부에 확산되거나 불법적인 용도에 사용되었음을 인정할 증거는 발견되지 않는 점
⑦ 입사지원자들의 개인정보를 처리하는데에 영리의 목적이 없었던 점
⑧ 제3자의 범죄행위를 직접적인 원인으로 하여 발생한 점

4. 옥션 사건

가. 사건개요

2008년 1월 4일부터 2008년 1월 9일까지 4차례에 거쳐 중국인 해커로 추정되는 이가 옥션의 데이터베이스 서버에 침입하여, 해당 서버에 저장되어 있던 옥션 회원 약 1천만명[1]

1) 옥션은 사건 발생 당시에는 고객정보 중 일부인 약 1천만건이 유출됐다고 밝혔지만, 2010년 3월 본 사건의 유출 피해자가 전체 회원인 약 1,800만명이라고 발표하였다.

의 성명, 주민등록번호, 주소, 전화번호, 아이디 등 개인정보가 유출되었다. 옥션은 2008년 2월 4일 이 사고를 경찰 및 관계기관에 신고하였고, 2008년 2월 5일 옥션 회원들에게 개인정보 유출 사실을 공지하였다.

나. 판결요지

정보통신서비스 제공자가 정보통신서비스를 제공하기 위해 이용자로부터 수집한 개인정보를 해킹으로 인해 도난당하였을 때 이용자들에 대한 손해배상 책임을 지기 위해서는, 정보통신서비스 제공자가 해킹 사고를 방지하기 위해서 선량한 관리자로서 취해야 할 기술적 · 관리적 조치 의무를 위반함으로써 해킹 사고를 예방하지 못한 경우여야 한다.

정보통신서비스 제공자가 해킹 사고 방지를 위해 취해야 할 선량한 관리자로서의 주의의무를 위반하였는지 여부를 판단하는 고려사항은 아래와 같다.

① 관련 법령이 정보통신서비스 제공자에게 요구하고 있는 기술적 · 관리적 보안 조치의 내용
② 해킹 당시 당해 정보통신서비스 제공자가 취하고 있던 보안 조치의 내용
③ 해킹 방지 기술의 발전 정도
④ 해킹 방지 기술 도입을 위한 경제적 비용 및 그 효용의 정도
⑤ 해커가 사용한 해킹 기술의 수준
⑥ 개인정보 유출로 인해 이용자가 입게 되는 피해의 정도

위와 같은 법리를 기초로 다음의 각 사항을 살펴보면, 옥션이 선량한 관리자로서의 주의의무를 위반한 점이 인정되지 않는다.

① 웹 서버인 이노믹스 서버 노출 주장
② 웹 방화벽 미설치 주장
③ 개인정보 암호화 미이행 주장
④ 인증 및 접근 제어 시스템 미도입 주장
⑤ 쿼리 미탐지 주장
⑥ 아이디 및 비밀번호 설정 주장
⑦ 해킹사고 부적절 대응 주장
⑧ 정보통신망법 제28조에 따른 손해배상 주장
⑨ 전자금융거래 이용약관 및 전자금융거래법에 따른 손해배상 주장

옥션은 이 사건 해킹사고 당시 다음과 같이 정보통신망법 등에서 규정하고 있는 개인정보보호를 위한 기술적 · 관리적 보호조치를 한 사실이 인정된다.

① 개인정보 관리계획의 수립 · 시행
② 업무요청시스템을 통한 개인정보처리시스템 접근 제어 및 접근 기록 저장
③ 침입탐지시스템 및 침입방지시스템 운용
④ 정보보호정책 및 관리지침 등을 통한 패스워드 작성 규칙 수립 · 시행, PC 보안 지침 수립 · 시행, 스팸 메일 · 인터넷 유해사이트를 차단하는 응용 소프트웨어 운영
⑤ 회원 비밀번호의 일방향 해쉬 알고리즘을 통한 암호화 저장, 개인정보 전송 구간의 SSL 암호화 송 · 수신
⑥ 복수의 백신소프트웨어 설치 · 운영, 업무요청시스템을 통해 사전 승인 후 개인정보 출력가능

5. GS칼텍스 사건

가. 사건개요

GS칼텍스는 이용실적에 따라 포인트가 적립되는 GS 포인트카드 회원으로 가입한 고객들의 개인정보를 데이터베이스에 구축하여 관리하고 있다. 그런데 동 데이터베이스에 접근할 권한이 있는 자회사 직원이 해당 권한을 이용하여 고객정보를 빼낸 후 이를 시중에 판매하거나 집단 소송을 의뢰받을 변호사에게 판매하는 방법 등으로 금원을 취득하기로 모의하였다. 2008년 7월 8일부터 2008년 7월 20일까지 데이터베이스 서버에 접속하여 회원 1,100만여명의 성명, 주민등록번호, 주소, 전화번호, 이메일 주소 등 개인정보를 자신의 사무용 컴퓨터로 전송받아 76개의 엑셀파일로 저장하였다.

공범 중 한 명이 2008년 8월 28일 한 변호사 사무실 사무장에게 1,200만명의 개인정보를 넘겨줄테니 집단소송에 활용하고 그 수익을 달라고 제의하였고, 사무장은 집단소송을 위해서는 우선 개인정보 유출 사실이 언론에 보도되어 사회문제가 되어야 한다고 말하였다. 이에 해당 공범은 2008년 9월 2일 기자들을 만나 '도심 쓰레기 더미에서 GS칼텍스 고객정보가 담긴 DVD를 주웠다'는 취지로 말하며, 개인정보가 담긴 CD와 DVD를 교부하였다. 2008년 9월 4일 한 기자는 건네받은 CD, DVD에 수록된 개인정보가 GS칼텍스 고객정보와 일치하는지 여부를 문의하였고, 2008년 9월 5일 GS칼텍스는 위 CD 및 DVD에 수록된 개인정보가 데이터베이스에 수록된 개인정보와 거의 일치함을 확인하였으며, 같은

날 “서울 도심 한복판 쓰레기 더미에서 1,100만 명이 넘는 개인정보가 담긴 ‘GS칼텍스 고객 명단’이라고 적힌 CD가 발견되었다”는 내용이 언론에 보도되었다.

2008년 9월 5일부터 2008년 9월 6일까지 사건 관련 공범들은 검거되었고, 공범들이 소지하고 있던 고객정보가 수록된 CD, DVD 등은 모두 압수되었거나 폐기되었다. 기자 등에게 제공된 CD 및 DVD는 언론보도 이후 전량 임의제출되거나 폐기 · 압수되었다.

나. 판결요지

정보통신서비스 제공자 등이 개인정보를 취급할 때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 기술적 · 관리적 조치를 하여야 할 주의의무가 있다고 할 것이다. 그러나 정보통신서비스 제공자 등에게 개인정보 누출로 인한 손해 배상책임을 지우기 위해서는 원고(피해고객)들의 개인정보가 외부로 누출됨으로써 불특정 다수에게 공개되어 이를 열람할 수 있는 상태 또는 원고들의 의사에 반하여 개인정보가 수집 · 이용될 수 있는 상태에 이르러 원고들의 개인정보자기결정권이 침해되었다거나 침해될 상당한 위험이 발생하였다는 점이 인정되어야 한다고 할 것이다.

이 사건의 경우 범행공모자가 고객정보를 빼내어 보관하던 저장매체나 기자들이 언론보도를 위하여 소지한 저장매체가 모두 조기에 수사기관에 제출되었거나 폐기된 점 등을 비추어 보면, 원고들의 개인정보가 불특정 다수에게 공개되어 이를 열람할 수 있는 상태 또는 원고들의 의사에 반하여 개인정보가 수집 · 이용될 수 있는 상태에 이르러 원고들의 개인정보자기결정권이 침해되었다거나 침해될 상당한 위험이 발생하여 원고들에게 정신적 손해가 발생하였다는 점을 인정하기 어렵다. 또한 원고들이 자신들의 개인정보가 추가로 복제되어 유출됨으로써 제3자에게 공개되거나 범죄 등에 도용 또는 악용될지도 모른다는 막연한 불안감이나 불쾌감을 가지게 될 수도 있었음은 능히 추단되나, 이러한 사정만으로 원고들이 수인한도를 초과하여 GS칼텍스가 금전으로 위자할만한 정신적 손해를 입었다고 평가하기는 어렵다. 따라서 GS칼텍스의 주의의무 위반 여부 및 위자료의 액수 등 나머지 점에 관하여 나아가 살펴볼 필요 없이 이유 없다.

Ⅳ. 금융권 시사점

개인정보 유출사고 발생시 해당 기업은 벌금 · 과태료 부과 및 경영진의 불구속 입건과 같은 형사적 책임[2], 개인정보 유출 피해자들에 대한 민사상 손해배상 책임, 그 외 규제당국의 간섭, 기업 이미지 하락, 고객 신뢰성 하락, 매출 감소 및 주식가치 하락 등 다양한 책임을 지게 된다.

따라서 본 장에서는 앞서 살펴본 개인정보 유출 관련 판례를 분석하여 유출기업의 여러 가지 책임 중 다양한 이해관계가 얽혀있고 사회적 파급효과가 큰 민사상 손해배상 책임에 대해 좀더 자세히 알아보고자 한다. 그리고 개인정보 유출기업의 책임에 대한 명확한 이해를 통해 개인정보 유출사고 발생시 책임을 최소화하고 고객의 개인정보를 안전하게 보호할 수 있는 효과적인 개인정보 위험관리 방안을 마련하고자 한다.

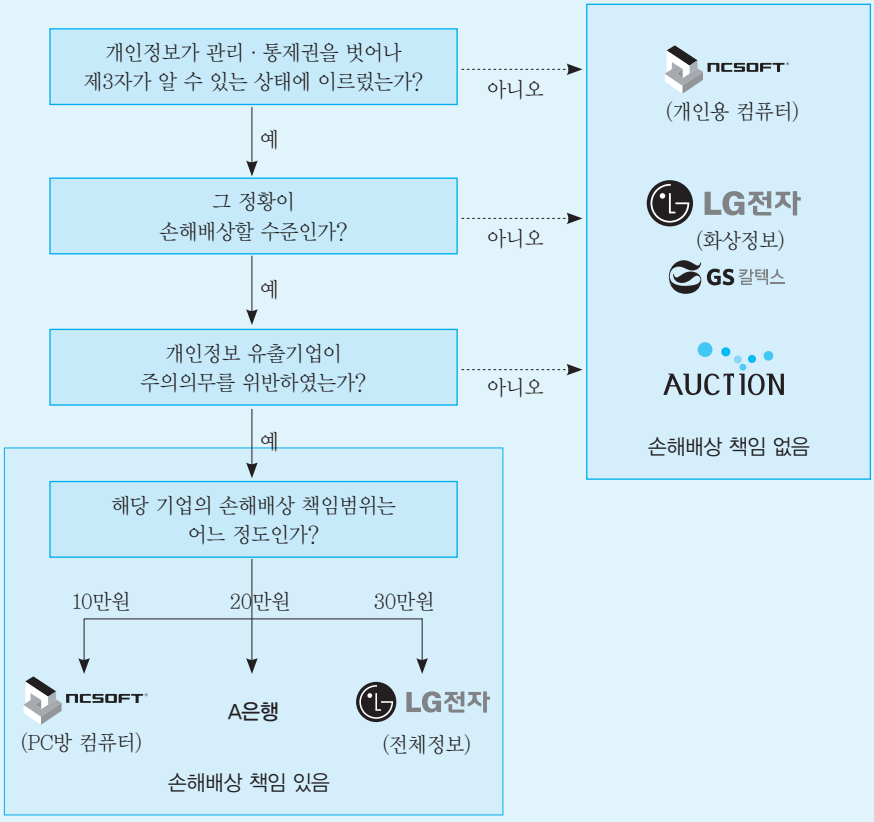
1. 개인정보 유출기업의 책임에 대한 이해

지금까지 살펴본 개인정보 유출 관련 판례를 분석해보면, 개인정보 유출기업의 책임을 정하는데 있어 주요 쟁점은 다음의 4가지라 할 수 있다(그림1 참조).

① 개인정보가 해당 기업 및 이용자의 개인정보 관리 · 통제권을 벗어나 제3자가 알 수 있는 상태에 이르렀는가?
② ①번이 그러하다면, 유출된 개인정보의 성격 및 확산범위 등 그 정황이 손해배상할 수준인가?
③ ②번이 그러하다면, 개인정보 유출기업이 선량한 관리자로서 지켜야할 주의의무를 위반하였는가?
④ ③번이 그러하다면, 해당 기업의 손해배상 책임 범위는 어느 정도인가?

2) 2010년 3월 신세계몰, 아이러브스쿨 등 25개 기업사이트에서 성명, 주민등록번호, 주소, 아이디, 비밀번호 등 약 2천만건의 개인정보가 해킹으로 인해 유출되었다는 사실이 밝혀졌다. 개인정보 유출기업들 중 개인정보를 안전하게 보호하기 위한 기술적 · 관리적 보호조치를 제대로 이행하지 않은 업체들이 처벌을 받았는데, 중요정보를 암호화하지 않은 업체 경영진들은 불구속 입건되었고, 개인정보처리자에 대한 보안교육을 실시하지 않은 업체들은 과태료 처분을 받았다.

〈그림1〉 개인정보 유출기업의 책임



첫번째 쟁점은 개인정보가 해당 기업 및 이용자의 개인정보 관리 · 통제권을 벗어나 제3자가 알 수 있는 상태에 이르렀는지, 즉 개인정보가 유출되었는지 여부이다. 이 때 제3자가 개인정보의 내용을 취득하여야만 유출되었다고 보는 것은 아니며, 일반적 수준의 제3자가 해당 정보를 알 수 있는 상태에 이르렀다면 개인정보가 유출된 것으로 본다. 엔씨소프트 사건에서는 동일한 개인정보인 아이디와 비밀번호가 기록되었다 하더라도, 기록된 장소가 PC방 컴퓨터인지 집의 개인용 컴퓨터인지에 따라 개인정보 유출 여부를 다르게 판단한 바 있다. 즉, PC방 컴퓨터의 로그파일에 아이디와 비밀번호가 기록된 경우는 컴퓨터에 관한 일정수준의 지식이 있는 제3자라면 누구라도 로그파일에 접근하여 해당 정보를 알 수 있는 상태에 이르렀으므로 개인정보가 유출된 것으로 인정하였지만, 개인용 컴퓨터에 기록된 경우는 개인정보 유출로 인정하지 않았다. 그리고 엔씨소프트 사건에서 개인용 컴퓨터에 기록된 경우를 제외하고 다른 모든 사건에서는 개인정보가 유출되었음을 인정하였는

데, 특히 화상정보(사진)가 개인정보인지 논란이 되었던 LG전자 사건을 눈여겨볼 필요가 있다. LG전자는 화상정보만으로는 개인의 식별이 불가능하다는 취지의 주장을 하였지만, '개인을 식별할 수 있는 정보'는 당해 정보에 의해 개인을 식별할 가능성만 있으면 되는 것으로, 화상정보는 성명 및 주민등록번호와 마찬가지로 개인정보라 인정되었다.

두번째 쟁점은 유출된 개인정보의 성격 및 확산범위 등을 고려할 때 그 정황이 금전으로 손해배상할 정도의 수준인가 하는 것이다. LG전자 사건에서 화상정보(사진)는 안전성 확보조치를 강구해야 할 개인정보라 할 수 있지만, 성명, 주민등록번호, 학력 등 입사지원을 위한 등록정보가 명백히 유출된 경우 외에 단지 입사지원자의 사진이 50명 단위로 화면에 노출된 경우(단순히 열람당할 가능성이 있는 경우)는 위자료 청구를 인정하지 않았다. GS칼텍스 사건에서는 유출된 개인정보가 범행 관계자 및 언론 등 소수의 수중에만 머물러 있다가 수사기관에 제출 또는 폐기되었기에, 불특정 다수에게 공개되어 이를 열람할 수 있는 상태 또는 의사에 반하여 개인정보가 수집 · 이용될 수 있는 상태에 이르렀다 인정할 수 없으므로, GS칼텍스가 금전으로 손해배상할 정도의 수준이 아니라고 판결되었다.

세번째 쟁점은 개인정보 유출기업이 선량한 관리자로서의 주의의무를 위반하였는지 여부이다. 해당 기업이 주의의무를 위반하였는지 여부를 판단하는 것은 법률적 판단이 개입될 수 있는 사안으로 논란의 여지가 있을 수 있다. 관련 판례에 따르면 법령이 요구하고 있는 기술적 · 관리적 보안 조치의 내용, 해킹 당시 취하고 있던 보안 조치의 내용, 해킹 방지 기술의 발전 정도, 해킹 방지 기술 도입을 위한 경제적 비용 및 그 효용의 정도, 해커가 사용한 해킹 기술의 수준, 개인정보 유출로 인해 이용자가 입게 되는 피해의 정도 등을 고려하여 주의의무를 위반하였는지 여부를 판단하고 있다(표3 참조). 옥션 사건에서는 이러한 법리를 기초로 옥션이 해킹사고 당시 개인정보보호를 위한 기술적 · 관리적 보호조치를 한 사실이 인정되며, 선량한 관리자로서의 주의의무를 위반한 점은 인정되지 않는다고 판결되었다.

〈표3〉 개인정보 유출기업의 주의의무 위반여부 판단시 고려사항

- 법령이 요구하고 있는 기술적 · 관리적 보안 조치의 내용
- 해킹 당시 취하고 있던 보안 조치의 내용
- 해킹 방지 기술의 발전 정도
- 해킹 방지 기술 도입을 위한 경제적 비용 및 그 효용의 정도
- 해커가 사용한 해킹 기술의 수준
- 개인정보 유출로 인해 이용자가 입게 되는 피해의 정도 등

네번째 쟁점은 개인정보 유출기업의 손해배상 책임 범위가 어느 정도인가 하는 것이다. 관련 판례에 따르면 손해배상 책임의 범위를 정함에 있어, 개인정보를 처리하는 자가 취한 사고 당시의 보안조치의 수준, 사고발생 후 얼마나 신속하게 사고를 파악하고 적시에 적절한 피해확산 방지조치를 취하였는지 여부, 피해자의 자기정보통제권과 관련하여 피해자에 대한 사고 발생 안내의 적절성 및 피해접수 내지 확인 · 피해회복조치 이행 여부, 유출된 정보의 성격 및 유출된 정보의 양, 정보가 유출된 범위 및 유출된 정보의 전파 가능성, 스팸메일이나 명의도용 등 추가적인 피해 발생 여부, 개인정보를 처리하는 자가 개인정보를 수집 · 처리함으로써 얻는 이익 등을 고려하고 있다(표4 참조). 엔씨소프트 사건, A은행 사건, LG전자 사건 등 각 사건 별로 10만원에서 30만원까지 다양한 위자료 판결을 받았음을 확인할 수 있다.

〈표4〉 개인정보 유출기업의 손해배상 책임 범위 책정시 고려사항

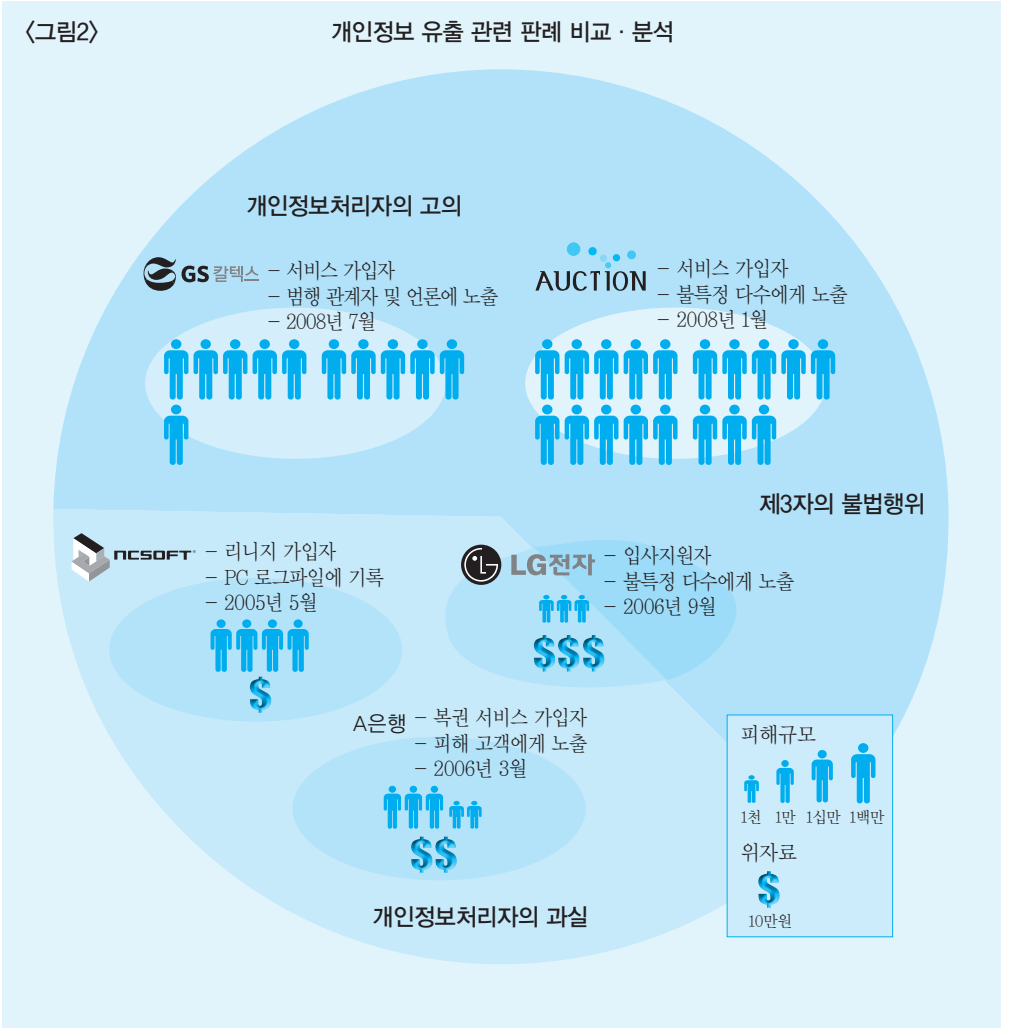
- 개인정보를 처리하는 자가 취한 사고 당시의 보안조치의 수준
- 사고발생 후 얼마나 신속하게 사고를 파악하고 적시에 적절한 피해확산 방지조치를 취하였는지 여부
- 피해자의 자기정보통제권과 관련하여 피해자에 대한 사고 발생 안내의 적절성 및 피해접수 내지 확인 · 피해회복조치 이행 여부
- 유출된 정보의 성격 및 유출된 정보의 양
- 정보가 유출된 범위 및 유출된 정보의 전파 가능성
- 스팸메일이나 명의도용 등 추가적인 피해 발생 여부
- 개인정보를 처리하는 자가 개인정보를 수집 · 처리함으로써 얻는 이익 등

이 같은 주요 쟁점들을 종합적으로 고려한 주요 개인정보 유출 관련 판례를 비교 · 분석하면 〈표5〉, 〈그림2〉와 같다.

〈표5〉 개인정보 유출 관련 판례 비교 · 분석

구분	엔씨소프트 사건	A은행 사건	LG전자 사건	옥션 사건	GS칼텍스 사건
사건 발생시기	2005년 5월	2006년 3월	2006년 9월	2008년 1월	2008년 7월
사건 발생원인	개인정보 처리자의 과실	개인정보 처리자의 과실	개인정보처리자의 과실과 제3자 (해커 등)의 불법 행위의 경합	제3자(해커 등)의 불법행위	개인정보 처리자의 고의
피해자	사고기간(약5일) 동안 리니지II 게임에 접속한 이용자	은행 복권서비스 가입자	LG전자 입사지원자	옥션 회원	GS칼텍스 고객
피해규모	약 40만명	32,377명	약 3,000명	약 1,800만명	약 1,100만명
유출정보의 성격	리니지II 게임 아이디 및 비밀번호	성명, 주민등록번호, 이메일주소 등	성명, 주민등록번호, 학력, 학점, 경력 등	성명, 주민등록번호, 주소 등	성명, 주민등록번호, 주소 등
유출 확산 범위	이용자PC의 로그파일에 기록	피해 고객 앞 이메일로 전송	불특정 다수의 인터넷 열람	중국인 해커로 추정되는 제3자 등 불특정 다수	범행 관계자 및 언론 등에 CD 및 DVD로 배포
유출기업의 주의의무 위반 여부	위반	위반	위반	위반 아님	–
유출기업의 손해배상 책임 여부	위자료 지급 (10만원)	위자료 지급 (성명, 주민등록번호, 이메일 유출시 20만원, 성명과 이메일 유출시 10만원)	위자료 지급 (30만원)	책임 없음	책임 없음
비고	PC방 컴퓨터의 경우만 개인 정보 유출로 보고, 개인용 컴퓨터의 경우는 개인 정보 유출로 인정하지 않음	–	단순히 열람당할 가능성이 있는 경우는 위자료 청구를 인정하지 않음	–	–

〈그림2〉 개인정보 유출 관련 판례 비교 · 분석



2. 개인정보 위험관리 방안 마련

금융기관은 개인정보 유출기업의 책임에 대한 이해를 토대로 개인정보 유출사고에 대비하여 효과적인 개인정보 위험관리 방안을 마련할 필요가 있다. 앞서 살펴본 바와 같이 개인정보 유출기업의 책임은 단순히 유출사고 발생 당시의 상황 뿐만 아니라 유출사고 발생 전후의 조치들에 의해서도 영향을 받는다. 즉, 해당 기업이 사고 발생 전 개인정보를 보호하기 위해 취하고 있던 조치들부터 사고 발생 후에 개인정보 유출 고객의 피해를 최소화하고 보상하기 위해 취한 조치들까지 모두 직 · 간접적으로 개인정보 유출기업의 책임에 영향을 주고 있다.

따라서 금융기관은 평상시에는 개인정보보호를 위하여 개인정보의 수집, 이용, 제공, 파기 등 단계별로 요구되는 보호기준을 준수하고, 기술적 · 관리적 · 물리적 보호조치를 충분히 이행하는 것은 물론 개인정보 영향평가를 통해 개인정보 유출 위험요인을 분석하고 개선사항을 도출하는 것이 필요하다. 또한 개인정보 유출사고에 대비한 대응 매뉴얼 등을 마련하여 개인정보 유출사고 발생시 최대한 사고를 빨리 탐지하고 신속하고 적절한 사후조치를 취함으로써 피해를 최소화하는 것이 중요하다.

그리고 유출사고 발생시에는 유출정보의 성격, 규모, 확산 범위, 유출로 인한 실질적인 피해, 전파 가능성, 추가 피해 발생 여부, 사고당시 취하고 있던 보호조치의 수준, 유출의 원인 등을 파악하고 관련 증거들을 수집하는 것이 필요하다. 이 때 관련 증거들이 법적으로 인정받을 수 있도록 변호사 자문 및 법무팀과의 협업 등을 통해 미리 준비할 필요가 있다. 또한 개인정보 유출사실을 인지하였을 경우 지체 없이 피해 고객에게 통지하고 개인정보 유출로 인한 피해 현황을 접수받을 수 있는 창구를 마련하는 것은 물론 신속하고 적절한 피해 확산방지 및 피해회복 조치를 통해 추가적인 피해를 최소화하고 피해 고객들의 권리를 구제하고자 노력해야 한다(표6 참조).

〈표6〉 **개인정보 위험관리 방안**

구분	위험관리 방안[주]
평상시 관리 항목	① 개인정보의 수집, 이용, 제공, 파기 등 단계별로 요구되는 보호기준을 준수 – 수집 목적, 항목, 보유 및 이용기간을 고지하고 정보주체의 동의 획득 – 필요 최소한의 개인정보를 수집 – 개인정보를 제3자에게 제공할 때에는 제공받는 자, 제공받는 항목, 보유 및 이용기간 등을 고지하고 정보주체의 동의 획득 – 개인정보가 불필요하게 되었을 때에는 지체없이 복구 또는 재생되지 않도록 파기 – 사상, 신념 등 사생활을 현저히 침해할 우려가 있는 민감한 정보는 처리를 제한 – 업무를 위탁할 경우에는 수탁자가 개인정보를 안전하게 처리하는지 감독하는 등 적절한 조치 – 개인정보 취급자에 대한 정기적인 교육 실시 등 ② 개인정보의 안전한 관리를 위해 요구되는 기술적 · 관리적 · 물리적 보호조치를 충분히 이행 – 개인정보 처리방침의 수립 및 공개 – 개인정보 보호책임자의 지정 – 개인정보 보호계획의 수립 및 시행 – 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 – 개인정보 유출 및 오 · 남용 방지를 위한 내부통제시스템의 구축 – 개인정보에 대한 접근 통제 실시 – 개인정보 접속기록의 위 · 변조 방지 조치 – 악성프로그램 방지 조치 등 ③ 개인정보 영향평가를 통한 개인정보 유출 위험요인 분석과 개선사항 도출 ④ 개인정보 유출사고에 대비한 대응 매뉴얼 등 마련 – 유출사고 발생시 확인 · 수집 · 조치한 사항들이 법적 증거로 인정받을 수 있도록 변호사 자문 및 법무팀과의 협업 등을 통해 준비 등

유출사고 발생시 확인 항목	① 유출정보의 성격, 규모, 확산 범위 ② 유출로 인한 피해의 정도 – 실질적인 피해 현황 – 유출된 개인정보의 전파 가능성 – 스팸메일이나 명의도용 등 추가적인 피해 발생 여부 등 ③ 사고당시 취하고 있던 보호조치의 수준 ④ 유출의 원인(해킹인 경우 해킹기술의 수준, 해킹방지기술의 발전정도, 해킹방지기술 도입을 위한 경제적 비용 및 그 효용의 정도 등도 함께 확인)
유출사고 발생시 조치 항목	① 개인정보 유출사실을 지체없이 피해 고객에게 통지 – 인터넷 홈페이지 상의 공지 뿐만 아니라 피해 고객에게 유선 및 이메일로 개별 통지 필요 ② 피해 고객으로부터 개인정보 유출로 인한 피해 현황을 접수받을 수 있는 창구 마련 ③ 신속하고 적절한 피해 확산방지 및 피해 회복조치 – 개인정보 유출을 야기한 직 · 간접적인 사고발생 원인 즉시 제거 – 미비한 기술적 · 관리적 · 물리적 보호조치 보완 – 유출된 개인정보의 악용 또는 도용을 막을 수 있는 대책 마련 등 ④ 유출사고로 인한 민 · 형사상 책임 등에 대한 법률 자문 및 대책 마련

주) 위험관리 방안의 세부적인 내용은 개인정보보호법을 바탕으로 한 시행령, 시행규칙, 관련 고시 및 지침 등을 통해 구체화될 예정

금융기관은 업무 특성상 고객의 개인정보를 많이 활용하고 있으므로 개인정보를 안전하게 보호하여 고객의 개인정보에 대한 권리와 이익을 보장할 의무가 있으며, 만약 개인정보가 유출된다면 민 · 형사상 책임을 비롯한 기업 이미지 하락, 매출 감소 등 다양한 책임을 지게 된다. 따라서 금융기관은 효과적인 개인정보 위험관리 방안을 마련하여 이행하는 등 고객의 개인정보를 안전하게 보호하기 위해 최선의 노력을 다하여야 한다.

〈참 고 문 헌〉

[1] 강신기, 개인정보보호법 제정경과 및 주요내용, 개인정보보호법 워크숍, 2011. 2

[2] 공공기관의 개인정보보호에 관한 법률, 법률 제10012호

[3] 구태언, 기업의 보안조치의무와 관련한 판례 동향, 제8회 인터넷 & 정보보호 세미나, 2010. 8

[4] 김지현, 최근의 판례로 비추어 본 개인정보보호 동향, 국제 개인정보보호 심포지움 2010, 2010. 3

[5] 신용정보의 이용 및 보호에 관한 법률, 법률 제10228호

[6] 임종인, 고객정보 유출로 인한 기업의 책임, 상장협연구 제59호, 2009. 4

[7] 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 법률 제10166호

[8] 행정안전위원회, 개인정보보호법안(대안), 2010. 9

[9] 개인정보 유출 관련 주요 판례

· 서울중앙지방법원 2007.1.26. 선고 2006나12182

· 서울고등법원 2007.11.27. 선고 2007나33059

· 서울고등법원 2008.11.25. 선고 2008나25888

· 서울중앙지방법원 2010.1.14. 선고 2008가합31411

· 서울중앙지방법원 2010.9.16. 선고 2008가합90021, 2008가합88370