준 비 서 면

사 건 2016가합680254 손해배상(기)
원 고 1. E
2. F
3. G
위 원고들 소송대리인 법무법인 정통, 담당변호사 정보호

피 고 주식회사 A
서울특별시 서초구 서초중앙로8길 OOO
대표이사
위 피고 소송대리인 법무법인 옳음, 담당변호사 나승소

원고 소송대리인은 위 사건에 관하여 다음과 같이 변론을 준비합니다.

다 음

1. 사건의 경위

1. 개인정보를 개인의 동의 없이 제3자에게 제공한 사실

피고 주식회사 A(이하 '피고')는 인터넷 쇼핑몰 B를 운영하는 회사이다. B는 이른바 오픈마켓 쇼핑몰로, 개인 또는 소규모업체가 직접 상품을 등록해 판매하는 웹사이트이다. 피고는 B쇼핑몰에서의 고객들의 구매 행태, 고객의 특성 등을 바탕으로 B의 사이트 배치개선, 상품 추천 등을 하고자 한다. 이에 빅데이터 분석이 필요하여 알고리즘 개발 목적으로 전체 가입자 중 최근 3개월 구매 횟수 기준 상위 200만명의 정보에서 ID, 성별, 나이, 거주지('동'까지 기재), 최근 3개월간의 구매내역을 추출하여 별도로 DB (이하 '이 사건 DB')를 작성하였다. 이를 위해 피고는 위 빅데이터 분석 작업을 C사에 위탁하였다. 위탁 시 피고는 홈페이지에 개인정보 처리방침에 대해 공개하였을 뿐 해당 고객들로부터 위탁사실에 관한 동의를 얻은 바 없다.

2. C사 개발담당자들에 대한 보안교육과 업무행위 상의 관리 및 감독에 관한 사실

C사 개발담당자 D에게는 피고의 DB시스템에 접근할 수 있는 망분리된 업무용 컴퓨터가 배정되었다. 프로젝트 진행 도중 D는 교통사고로 병원에 입원하게 되었고, D는 개발업무 수행이 가능한 유일한 사람이었기에 피고는 내부 결재를 통해 VPN 사용을 승인하고 병원에서 D의 노트북으로 개발업무를 계속하도록 허용했다. 피고는 위탁업무를 수행하는 C사의 직원들에게 프로젝트 시작 전 1회 보안교육을 시행하였으나 구체적으로 업무행위를 감독하지는 않았다.

3. 해킹사실에 대한 늦은 통지 및 신고

해커가 2016. 7. 23. A의 이 사건 DB를 해킹하여 그 안에 저장되어 있던 정보를 자신의 PC로 1회 다운로드한 사고가 발생하였고, 피고는 2016. 7. 24. 해킹 사실을 확인하였으나, 정확한 사실관계를 파악하기 위해 자체조사 하다 2016. 8. 1. 해킹사실을 이용자에 통지하고 이를 한국인터넷진흥원에 대하여 신고하였다.

4. 해킹의 방법

해커는 인터넷에서 쉽게 다운로드 받을 수 있는 비상업용 무료 프로그램에 백도어 프로그램을 포함했고, 업무수탁자 C의 개발담당자 D가 그 프로그램을 개인적 용도로 사용하기 위한 개인 노트북에 다운로드 받자 노트북에 위 백도어 프로그램이 설치되었다. 개발담당자 D가 병원에서 작업하기 위해 VPN으로 피고의 전산망에 접속하자 노트북을 장악한 해커가 DB시스템에 접근해 이 사건 이 사건 DB의 정보를 덤프(dump)파일로 생성하고 다운로드 받았다. 해킹에 의한 파일 생성 및 다운로드는 2016. 7. 23. 오전 3시부터 4시 30분까지 이루어졌으며 다운로드 된 개인정보 데이터 크기는 대략 3GB에 달한다.

5. 미래부고시에 따른 의무를 이행하지 않은 사실

피고는 미래창조과학부고시 제2013-196호 '정보보호조치에 관한 지침' (이하 "미래부고시"로 한다) 별표 1에 따라 '네트워크 모니터링 도구를 이용하여 백본망, 주요 노드 및 외부망과 연계되는 주요 회선의 트래픽 소통량을 24시간 모니터링'할 수 있음에도 불구하고 이 사건 DB의 다운로드와 관련한 트래픽 모니터링을 하지 아니하였다. 또한 피고가 정보보호를 위해 집행한 예산은 2%에 지나지 아니하였다.

6. 피고는 방송통신위원회 고시 제2015-03호 '개인정보의 기술적-관리적 보호조치 기준'(이하 "방통위고시"로 한다)에 의거하여 망분리 의무대상자에 해당한다. 피고는 내부 개발실에 있던 업무용 컴퓨터는 내부 방침상 모두 망분리 해둔 상태였으나, 피고는 빅데이터 분석 알고리즘 개발 DB를 개발이 완료되지 않은 관계로 개인정보처리시스템으로 분류하지 않았다.

7. 침해사고 이후의 경위

다운로드 받은 정보는 이미 삭제된 상태고, 해커는 오로지 재미로 해킹을 시도해 본 것일 뿐 정보는 모두 폐기하였다고 주장하고 있으며, 정보의 사용 여부, 추가 복제 여부, 공범의 존재, 제3자에 대한 전달 여부에 관하여도 부인하고 있다. 이러한 진술을 입증 또는 반박할 만한 추가 증거는 발견되지 아니한 상태이다.

원고 E, F, G(이하 '원고들')는 B 사이트의 회원으로 2016. 8. 1. 피고로부터 개인정보유출통지를 받았다. B사이트를 통해 당시 위암 수술을 한 원고 E는 "위암을 이겨낸 사람들", "위암 수술 후 식사 가이드", "암 치료 후 건강관리 가이드" 등의 서적을 집중적으로 구매한 자이고, 2016. 2. 아이를 출산한 원고 F는 남아용 기저귀, 젖병세정제, 물티슈 등을 구매하고 있

었다. 원고 G는 2016. 2. 15. 스마트 TV, 냉장고, 세탁기를 구매한 바 있다.
2. 주위적 청구인 정보통신망법 제32조 제2항 위반에 관하여

피고는 개인정보 유출을 방지할 주의의무가 있음에도 이를 하지 아니한 중과실이 있는바, 그에 따라 이 사건 개인정보를 유출하여 원고들에게 손해가 발생하여 정보통신망법 제32조 제2항에 따라 손해배상을 청구하는바 그 근거는 다음과 같습니다.

가. 피고의 개인정보 유출에 대한 중과실

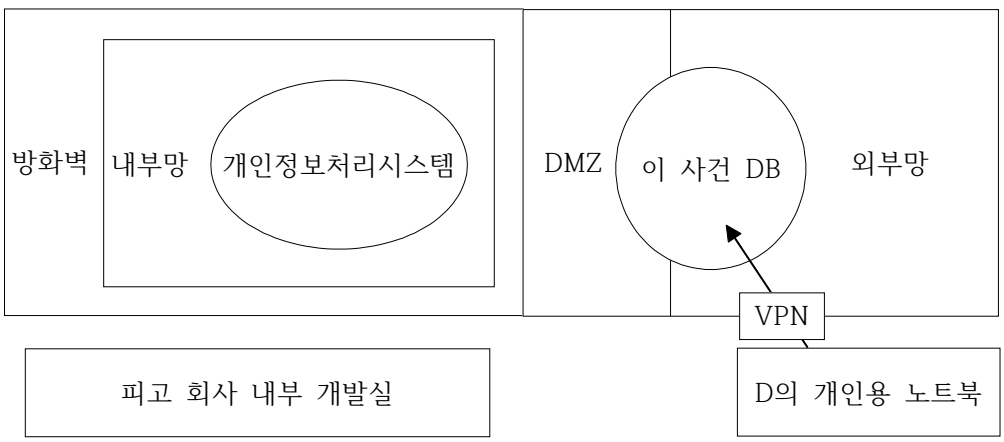
1) 개인정보의 유출을 방지할 주의의무의 위반

가) 정보통신망법 제28조제1항 및 같은 법 시행령 (이하 "시행령") 제15조제6항에 따른 방통위고시의 망분리 조치 의무의 위반

(1) 피고는 방통위고시에서 규정한 개인정보의 누출을 방지하기 위하여 취하여야 하는 기술적•관리적 조치를 다 하였다고 주장합니다. 그러나 확인된 사실관계에 의하면 피고는 이용자들로부터 수집된 개인정보에 대한 망분리 조치는 시행하고 있었으나 이 사건 빅데이터 알고리즘 개발을 위하여 만든 이 사건 DB는 망분리 대상으로 분류하지 않았는바, 결과적으로 망분리 의무 조치를 다하지 않은 중과실이 있는 것으로 보입니다.

방통위고시 제4조제6항에 따르면 "정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다."고 규정하고 있는 바, 개인정보처리시스템이란 같은 고시 제2조제4호의 정의에 따라 "개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템"입니다. 그러므로 이 사건 DB 또한 개인정보처리시스템에 속해야하는 점은 의문의 여지가 없음에도 불구하고, 피고는 이 사건 DB를 기존의 개인정보와 같이 보관해야하는 중요 정보로 생각하지 않는 등 이를 개인정보처리시스템에 포함시키지 않은 중대한 과실이 있습니다.

(2) 피고의 항변에 대한 재항변



피고는 내부개발실의 컴퓨터를 망분리 한 것으로 그 이행의무를 다하였다고 주장할 것으로 보입니다. 그러나 방통위고시에 따른 망분리 의무를 이행하였는가를 판단하는 데에 있어서는 피고가 '실질적'으로 이 사건 개인정보 유출을 막기 위한 기술적•관리적 보호조치 의무를 다하였는가를 검토해야합니다. 피고는 필수적으로 망분리 조치되어야 하는 이 사건 DB를 개인정보처리시스템에 포함시키지 않음으로써 망분리 조치가 실질적으로 이루어지지 않았는바, 이는 위의 그림에서 보는 바와 같습니다.

또한 이 사건에서 피고는 D에게 가설사설망(이하 "VPN")을 통해 외부로부터의 접속을 막고 D로만 하여금 이 사건 DB에 접근할 수 있도록 하여 방통위고시에 따른 논리적 망분리를 하였다고 주장합니다. 그러나 확인된 사실관계에 의하면 이 사건 해커는 VPN 자체를 해킹하여 개인정보를 유출시킨 것이 아니고 D의 개인용 노트북 즉, 자체적인 단말기를 이용하여 개인정보에 접근하였으므로 논리적 망분리가 무용지물이 되었다고 할 것입니다. 그리고 이러한 논리적 망분리의 취약성 및 피고가 논리적 망분리를 충분히 하였는지를 떠나서 피고는 이 사건 DB를 개인정보처리시스템에 포함시키지 않음으로써 피고가 이행하였어야할 물리적 망분리 조치의무를 다하지 않은 것만으로도 이는 침해사고에 대한 피고가 명백한 중과실이 있음을 증명합니다.

한편 피고는 정보통신망법 제28조제1항에서 및 방통위고시에 따라 요구되는 조치들, 즉 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립•시행, 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치•운영, 접속기록의 위조•변조 방지를 위한 조치, 개인정보를 안전하게 저장•전송할 수 있는 암호화기술 등을 이용한 보안조치, 백신 소프트웨어의 설치•운영 등 컴퓨터바이러스에 의한 침해 방지조치, 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치를 다하였기에 중과실이 없다고 주장할 것으로 보입니다. 그러나 보안유지의 업무 특성상 위 법령 등에서 요구되는 모든 조치들이 유기적으로 조화를 이뤄 하나의 완벽한 보안 체계를 유지되어야 합니다. 만일 그 중 하나라도 이행이 되지 아니한다면 그 보안망에 치명적인 흠이 생긴다는 점, 피고가 이 사건 DB를 개인정보처리시스템에 포함시키지 않은 행위는 개인정보 보호를 위한 여러 기술적•관리적 보호조치 중에서도 가장 큰 핵심을 이루는 보호조치라는 점 등을 미뤄봤을 때, 피고는 현저히 그 주의의무를 위반하였다는 책임을 피해갈 수 없을 것으로 보입니다.

나) 미래부고시 준수의무의 위반

피고는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하지 않은 데에 중과실이 있습니다. 미래부고시 별표1 중 피고가 이행하지 않은 부분들은 다음 도표에서 보는 바와 같습니다.

관리적 보호조치	1.8. 정보보호 투자	1.8.1. 정보보호 투자 계획 수립.이행	▸기업의 정보보호를 위해 위험관리에 기반한 적정 수준(정보기술부문 예산의 5% 이상)의 정보보호 예

			산 편성 및 집행
기술적 보호조치	2.1. 네트워크 보안	2.1.1. 트래픽 모니터링	▸네트워크 모니터링 도구를 이용하여 백본망, 주요노드 및 외부망과 연계되는 주요회선의 트래픽 소통량을 24시간 모니터링

(1) 피고가 관리적 보호조치로써 정보보호를 위하여 집행한 예산은 미래부고시의 규정과는 달리 정보기술부문 예산의 2%에 불과한 점

피고가 정보보호를 위해 편성•집행한 예산은 미래부고시에서 '기업의 정보보호를 위해 적정 수준 즉 정보기술부문 예산의 5%를 편성•집행하도록 하는 규정'에 미달하였습니다. 피고 회사의 재산규모 등의 파악이 힘들지만 피고 회사가 운영하는 B 사이트의 이용자가 1500만 명에 이르는 점을 미루어 보았을 때 피고가 미달한 3%의 예산은 매우 큰 액수에 해당할 것으로 보입니다. 그리고 거대한 규모의 개인정보를 보유하고 있으면서 정보보호 투자에 대한 관리를 매우 소홀히 한 점은 피고가 이 사건 침해사고를 방지하지 못한 것에 중대한 과실이 있음을 보여줍니다.

(2) 피고는 기술적 보호조치로써 네트워크 보안을 위해 24시간 트래픽 모니터링을 할 수 있었음에도 이를 전혀 이행하지 않은 점

정보통신망법 제45조와 이에 따른 미래부고시 별표1에 의하여 정보통신서비스 제공자는 침입차단시스템, 침입탐지시스템 등 정보보호시스템을 설치.운영하고 네트워크 모니터링 도구를 이용하여 주요 회선의 트래픽 모니터링을 할 기술적•관리적 보호조치를 취할 의무가 있습니다.

피고는 개인정보가 보관된 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역을 감시하고, 통상적으로 수행되는 업무와 다른 형태의 업무가 수행되거나 비정상적인 트래픽이 발생할 경우 이를 탐지하여 조처할 수 있도록 적절한 침입차단시스템과 침입방지시스템을 갖출 의무가 있습니다. 그러나 이 사건에서 해커가 약 200만 명에 이르는 회원의 개인정보를 유출하는 과정에서 3GB의 대규모 데이터 전송이 발생하였음에도, 이를 탐지하거나 차단할 수 있는 트래픽 모니터링 조치를 하지 않았으므로 이에 중대한 과실이 있습니다.

판례에 따르면 (서울고등법원 2013나20047 판결) 정보통신서비스 제공자는 방통위고시 제4조제5항제2호에 따라 개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보유출시도를 탐지하는 기능을 포함한 시스템, 즉 침입탐지시스템을 설치•운영하여야 한다고 판시하고 있는바, 이러한 침입탐지시스템에는 모니터링이 탐지의 전제가 된다는 의미에서 이 사건 DB 서버에서 외부로 유출되는 정보에 대한 트래픽 모니터링 의무가 당연히 포함된다는 점을 간과해서는 안 될 것입니다. 트래픽 모니터링은 개인정보 유출시도를 탐지하기 위한 최소한의 전제로서 보편적, 일반적으로 당연히 운영해야할 의무가 있는 것이고

이는 방통위고시에서도 인정되는 의무라고 볼 수 있는데 피고는 이러한 트래픽 모니터링을 전혀 하지 않은 중대한 과실을 저질렀습니다.

이 사건 해킹사고 당시 약 200만 명 회원의 개인정보가 유출되는 동안 대규모 데이터 전송이 발생하였을 것으로 예상되는 바, 피고가 이상징후를 트래픽 모니터링하고 이 사건 DB 서버와 관련된 IP주소, 트래픽 등을 분석하였다면 개인정보에 대한 복사명령, 전송명령이 이루어지는 것을 파악하여 정보유출을 충분히 막을 수 있었을 것입니다. 그러나 피고가 이 사건 침해사고 당시 이러한 기능을 사용하지 아니하여 트래픽이 많지 않은 새벽시간 (오전3시부터 4시30분)에 3GB에 해당하는 개인정보가 외부로 유출되는 것을 발견하지 못하였는바, 이는 피고가 보안관제정책을 완화하여 명백한 위험징후인 이 사건 DB 서버에서의 대용량 트래픽을 트래픽 모니터링하거나 탐지해야 할 기술적.관리적 보호조치를 전혀 이행하지 아니한 잘못 때문이라고 할 것입니다.

(3) 피고의 항변에 대한 재항변

피고는 피고가 방통위고시에 따른 기술적•관리적 보호조치를 모두 이행하였고 원고들이 주장하는 위 미래부고시 사항은 권고조치에 불과할 뿐이기에 법령상•계약상 의무를 위반하지 않았다고 주장할 것으로 보입니다.

한편 방통위고시 제1조제2항에 따라 정보통신서비스 제공자등은 사업규모, 개인정보 보유수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다고 규정되어 있습니다. 피고는 1500만명에 이르는 이용자들의 개인정보를 보유하고 있는 회사로써 그 사업규모 등을 고려할 때 높은 수준의 기술적•관리적 보호조치가 요구된다고 할 수 있습니다. 위 방통위고시에 따른 예산집행 기준 혹은 트래픽 모니터링 의무가 정보통신망법 시행령 상 권고조치로 되어있다 하더라도, 개별의 사업규모 등의 사정을 고려하지 않은 채 위 보호조치를 취하지 않은 것은 미래부고시의 고시 목적을 잠탈하고 피고의 중과실이 용인되는 결과를 낳을 것입니다.

다) 개인정보보호법 제28조 및 정보통신망법 제25조제4항에 따른 수탁자 C에 대한 관리감독의무 위반

피고는 개인정보보호법 제28조 및 정보통신망법 제25조제4항에 따라 수탁업자인 C 및 개발담당자 D에 대한 관리감독의무가 있는바, 피고는 이 관리감독의무를 현저히 위반하였습니다. 피고는 C사와 개인정보의 안전한 관리에 관한 특별한 약정을 하지 않았습니다. 피고가 C사와 특별한 약정을 하여 C사에 개인정보의 안전한 관리를 위하여 조치를 하도록 요구하고 그와 함께 개인정보 유출을 피하기 위한 조치를 하게 할 수 있었음에도 그러지 아니하였으므로, 이에 대하여 관리감독 의무를 위반하였다고 할 것입니다. 또한 방통위고시 제3조제2항은 정보통신서비스 제공자등은 개인정보관리책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 실시하여야 한다고 규정하고 있습니다. 그러나 피고가 D를 포함한 C사 직원들에게 일회성의 보안교육만을 시행한 점 등을 보아서도 피고는 C사의 직원인 D가 개인정보 보호를 위한 충분한 조치를 다 취하도록 관리•감독하지 않은 중과실이 있습니다.

피고는 C사에게 보안서약서를 징구하였고 D가 동종업무를 수차례 경험한 전문가로서 보안의 중요성을 충분히 인지하고 있던 터라 D에 대한 별도의 관리•감독이 필요하지 않았다고 항변할 것으로 보입니다. 그러나 이러한 보안서약서를 징구하였다는 사정만으로 피고가 C 및 D에 대한 관리•감독의무를 하였다고 말할 수는 없을 것입니다. 우선 이 사건 침해사고가 발생한 점에서 D가 개인용 노트북을 사용하였다는 점, 이에 대해 보안의 취약점이 드러났다는 점이 D에게 관리•감독의무를 하였어야 하는 점을 반증합니다. 그리고 비상업용 프로그램을 잘못 설치함으로써 보안 사고가 났던 선례가 있음에도 불구하고 개발담당자인 D가 유사한 잘못을 저지르게 한 점을 보았을 때, 업무용 컴퓨터에 개인적으로 사용하는 비상업용 프로그램을 설치하는 것을 금지하는 규정이나 교육 즉, 관리•감독이 없었음이 분명합니다.

2) 피고의 침해사고에 대한 인식가능성 및 회피가능성이 없을 것이라는 점에 대한 항변

(가) 피고는 해커가 D의 접근 권한을 토대로 이 사건 DB에 접근하였기 때문에 피고가 기술적•관리적 보호조치를 모두 준수하였더라도 이 사건 침해사고를 인식하거나 회피할 가능성이 없었다고 주장할 것으로 보입니다. 그러나 앞서 살펴본 바에 따르면 피고는 개인정보처리시스템에 이 사건 DB를 포함시키지 아니한 중대한 과실이 있고, 이러한 주의의무 위반이 없었다면 애초에 D의 권한을 이용하여 접근하는 사태도 막을 수 있었을 것입니다.

(나) 또한 미래부고시에 따른 트래픽 모니터링 조치의무를 준수하였다면 이 사건 침해사고를 미연에 방지할 수 있었을 것입니다.
먼저 ① 이 사건 침해사고가 발생한 시각은 트래픽량이 많지 않은 새벽3시에서 4시반사이였고 이 시간대에 3GB 정도의 트래픽이 발생하는 것은 이상 징후라고 충분히 판단될 수 있었을 것, ② 피고가 원용한 판례에 따르면 2GB, 2GB, 6GB에 이르는 3회 개인정보데이터 유출은 그 양이 매우 적어 트래픽 모니터링으로 감지할 수 없었다고 보았는바, 판례는 개인정보의 양에 집중하여 그 개수가 엄청나다는 점을 간과하였다는 점에서 문제가 있다고 할 수 있습니다. 개인정보의 데이터가 대체로 1인 당 1~10Kb에 불과하므로 3GB에 이르는 데이터의 개수는 실제로 엄청나게 많다는 점, 그래서 해커가 이 사건 DB 내를 계속하여 탐색 및 복사하는 과정에서 수많은 트래픽이 발생했을 것이라는 점, 그리고 현대의 정보보호기술 수준에 미루어볼 때 이 정도의 트래픽은 트래픽 모니터링을 통해 감지할 수 있었을 것이라는 점을 고려할 때 피고는 트래픽 모니터링을 하였더라면 이 사건 침해사고를 막을 수 있었다고 보아야 합니다. 마지막으로 ③ 피고는 1500만명의 개인정보를 보유하고 있는 업체이고 최소한의 보안을 위해서 트래픽 모니터링은 필수라는 점, 이와 유사한 해킹을 막을 수 있는 방법은 트래픽 모니터링이 유일하다는 점 등을 고려했을 때 피고에게는 중대한 과실이 존재하고, 트래픽 모니터링을 하지 않았어도 이 사건 침해사고를 인식하거나 회피할 수 없었을 것이라는 주장은 타당하지 못합니다.

나. 손해의 발생

1) 정보통신망법 제32조제2항 징벌적 손해배상의 청구

정보통신망법 제32조제2항은 "....이용자에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다"고 규정하는바 같은 조 제3항의 사항 등을 보았을 때 원고들은 피고로부터 3,000,000원을 손해배상액으로 청구하는 바 이에 대한 근거는 다음과 같습니다.

이 사건의 손해배상액 산정에 관하여 보건대, ① 피고는 기술적•관리적 보호조치를 충분히 이행함으로써 이 사건 침해사고를 막을 수 있음을 알 수 있었음에도 알지 못한 중대한 과실이 있으며, ②이 사건 해킹사고로 유출된 원고들의 개인정보는 아이디, 성별, 나이, 거주지, 그리고 3개월간의 구매내역 등의 정보이고 이들은 정보주체의 식별과 직접적으로 연결된 정보인 점, 이 사건 해커가 원고들을 비롯한 피고 회원들의 개인정보를 유출한 목적은 불분명하지만, 이 사건 해킹사고 당시는 물론 현재까지 개인정보가 상업적인 목적으로 광범위하게 수집 및 활용될 가능성이 있으며, 이 사건 해커가 위와 같이 유출한 개인정보를 제3자에게 판매하여 이익을 얻고자 하였을 가능성이 상당하고, 따라서 유출된 원고의 개인정보가 이미 광범위하게 확산·전파되었거나, 앞으로도 계속적으로 확산 및 전파될 가능성 또한 상당한 점, 해킹 사고 이후 원고들은 유출된 자신의 개인정보가 거래되거나 전파되고 있을 수 있다는 불쾌감은 물론 앞으로도 계속적으로 이에 추가 유출 피해 발생에 대한 불안감 등의 심리적·정신적 고통을 겪어야 하는 점, ③ 피고는 이 사건 정보통신망법 제28조 등의 위반으로 같은 법 제64조의3 제6호에따라 매출액의 100분의3이하에 해당하는 금액을 과징금으로 부과받을 것이 예상되는 점, ④ 피고는 원고들을 포함하여 무려 1500만명에 이르는 대규모 개인정보를 수집하고 있었음에도, 앞서 본 바와 같이 침입탐지시스템 등을 제대로 갖추지 아니하여 대용량의 개인정보가 파일로 생성되고 외부로 유출되는 것을 탐지하지 못하고, 방치하는 등 여러 면에서 개인정보를 보호할 의무를 소홀히 하여 이 사건 해킹사고를 방지하지 못한 점, ⑤ 피고가 피고 자신의 중대한 과실이 초래한 이 사건 침해사고 이후 이용자들의 피해구제를 위해 노력하지 않고 오히려 기술적•관리적 보호조치를 다하였음을 들어 피해구제를 거부하고 있는 점 ,⑥ 피고가 개인정보를 수집한 목적, 이를 수집한 방법 및 경위, 피고의 경제적 지위, 대규모 개인정보를 수집 및 보유하고 있던 정보통신서비스 제공자로서의 피고의 사회적 책임 등의 제반 사정을 종합적으로 고려해보면, 이 사건 해킹사고로 원고들이 입은 정신적 손해를 배상할 의무가 있는 것이고, 이 사건 침해사고로 원고들이 입은 정신적 손해배상에 대한 액수는 1,000,000원이 타당합니다. 판례(대구지법 2014.2.13. 선고, 2012나9865)에서도 이러한 기준에 의해 1,000,000원의 위자료를 인정한 바 있습니다. 그러나 정보통신망법 제32조제2항에서 법원은 손해액의 3배를 넘지 않는 범위에서 손해배상액을 정할 수 있다고 하고, 피고가 이 사건 침해사고를 방지하지 못한 과실이 매우 중대하므로 이를 3,000,000원으로 청구함이 타당하다고 생각됩니다.

2) 피고의 항변에 대한 재항변

피고는 이 사건 DB가 암호화되어 있었기 때문에 해커가 개인정보를 빼내었다 할지라도 정보의 사용가능성 등이 없어 원고들에게 손해가 발생하지 아니하였다고 항변할 것으로 예상됩니다. 그러나 유출된 개인정보의 악용가능성 등이 없었다는 사실을 불문하고 원고들이 개인정보유출을 통지받음으로 인해 심리적, 정신적 고통을 받았다는 점에 대해서는 변하는 사실이 없습니다. 현대사회에서 개인정보와 개인정보의 보호가 가지는 무게감은 날이 갈수

록 중해짐에도 피고의 위와 같은 중과실로 인해 이 사건 침해사고가 발생함에 따라 원고들이 얻은 불쾌감, 불신감 등은 이 사건 DB가 암호화되어 있었다는 점을 불문하고 이 사건 DB가 유출된 점에 기인한 정신적 손해라고 할 것입니다.

한편 피고가 원용하고 있는 손해배상책임을 부정한 판결들 중 대법원 2012.12.26. 선고 2011다59834 판결의 경우의 사안은 이 사건 침해사고와는 달리 개인정보 유출이 DVD, CD 등을 통해 이루어져서 데이터로 전송된 것과 달리 개인정보 유출이 현재적이지 않다는 점에서 그러한 판시를 한 것으로 보이므로 이와는 다르다고 보입니다.
또한 관련 법령에서 정한 기술적 관리적 보호조치의 내용, 피고가 이행한 기술적, 관리적 보호조치의 수준, 이 사건 해커가 사용한 해킹의 수법, 해킹 방지 기술의 한계, 해킹 방지 기술 도입을 위한 경제적 비용 및 그 효용의 정도 등을 종합적으로 고려하는데, 이 사건의 경우 피고는 해커가 2016. 7. 23. 해킹하여 다운로드하였음에도 만하루가 지나서 파악한 점, 새벽시간에 비정상적인 트래픽이 발생하였음에도 이를 전혀 탐지 못한 점, 업무수탁자 개인용 컴퓨터로 피고 전산망에 접근하여 일을 처리하게 함에도 업무수탁자 개인용 컴퓨터에 보안프로그램 등 설치를 하지 않는 등의 관리의무를 소홀히 한 점 등을 고려해보았을 때 피고가 명목상으로는 관련 법령에 따라 기재된 보호조치의 각 항목에 해당하는 조치를 모두 이행했다고 하더라도, 그 실질적인 보호의 수준이 매우 부족하거나, 적어도 이를 적절하게 관리, 운영하지 못한 것이라고 보아야 할 것입니다.

다. 소결

피고는 정보통신망법 및 동법 시행령 및 이에 따른 방통부고시와 미래부고시에 규정된 의무를 위반함에 있어서 중대한 과실을 저질렀고 이 사건 침해사고를 미연에 방지하지 못하여 원고들에게 정신적인 손해를 발생시켰으므로, 이에 따라 정보통신망법 제32조 제2항에 따른 손해배상책임을 지는바 원고들 각각에 대하여 3,000,000원의 손해를 배상하는 판결을 구합니다.

3. 예비적 청구에 관하여

피고는 원고들로부터 서비스 이용계약에 따른 개인정보를 제공받은 계약당사자, 또는 정보통신망법에 따라 정보통신서비스 이용자인 원고들의 개인정보를 취급하는 정보통신서비스 제공자로서 피고가 보유하고 있는 원고들의 개인정보가 분실.도난.누출.변조되지 않도록 개인정보를 보호.관리하고 그에 필요한 기술적 및 관리적 조치를 다하여야 할 주의의무가 있습니다. 그러나 피고는 다음과 같이 그 의무를 위반하여 이 사건 해킹사고를 미연에 방지하지 못하고 이를 통해 원고들의 개인정보가 유출되도록 하여 손해를 발생시켜 이용계약상 의무 위반 및 정보통신망법 제32조제1항에 따른 손해배상책임을 지는바, 이를 대신하여 제32조의2에 따른 법정손해배상을 청구하고 이에 대한 근거는 다음과 같습니다.

가. 예비적 청구 중 이용계약상 의무 위반에 관하여

(1) 이용계약상 개인정보보호 부수의무

개인정보보호법 제3조 제4항 및 제29조 등에서 정한 개인정보처리자로서의 일반적인 주의의무, 개인정보보호법 제28조에서 규정한 개인정보처리자의 개인정보취급자에 대한 관리감독의무, 피고의 업무와 그 목적 등을 종합해보면 피고와 원고들과의 계약관계에서 원고들이 개인정보를 제공하고 피고는 원고들로부터 제공받은 개인정보를 안전하게 보호하여야 하는 보호의무 내지 안전의무가 인정된다 할 것이며, 이는 이용 계약상 추구하는 목적을 달성하는데 필요한 일종의 부수의무의 성격을 가진다 할 것이다. 이에 따라 피고에 대해 원고들에 대한 부수의무로서의 보호의무 내지 안전의무를 위반하였다는 이유로 민법 제390조의 채무불이행책임이 인정될 것으로 보입니다. 또한 판례(대구지법 2014.2.13. 선고, 2012나9865)에 따르면 개인정보 해킹유출에 따른 손해배상을 구하는 경우에 정보통신망법 제32조에 따른 손해배상책임은 물론 계약상 채무불이행에 따른 손해배상책임도 부담한다고 보고 개인정보를 취급하면서 안전성 확보에 필요한 합리적인 수준의 기술적 및 관리적 대책을 수립·운영할 계약상 의무가 있다고 합니다.

이에 따라 채무불이행의 법리에 따르면 C사와 C사의 개발담당자인 D는 피고와 위탁용역계약을 체결한 개인정보 취급자로서 개인정보 처리자인 피고와의 관계에서 민법 제391조의 이행보조자에 해당한다고 볼 수 있는바, 이 사건에서 C사와 C사의 개발담당자인 D의 고의 및 과실은 곧 피고의 고의 및 과실로 취급된다고 할 것입니다. D는 개발담당자로서 보안업무의 기본을 준수해야할 주의의무가 있고 개인노트북이 아닌 망분리된 업무용 컴퓨터를 사용하여야 하는 점 및 개인노트북으로 업무를 볼 경우에 백신 및 바이러스 감지 프로그램을 설치하여 업무 보안의 안전을 도모해야할 주의의무가 있었는데 이를 게을리한 과실이 있다고 할 것이고, 이러한 이행보조자 D의 과실은 곧 민법제391조에 의해 피고의 과실로 볼 수 있는 것입니다. 따라서 피고에게는 이용계약상 채무불이행으로 인한 손해배상의 책임이 있습니다.

(2) 피고의 항변에 대한 재항변

피고는 개인정보 보호에 있어서 방통위고시에 따른 조치만 이행한다면 계약상 의무를 다한 것이라는 판례의 기준에 따라, 피고가 모든 계약상 의무를 다하였다고 주장할 것입니다.

그러나 위 주위적 청구에서 주장한 바와 같이 피고가 방통위 고시의 망분리 조치를 이행하였는가를 판단함에 있어서는 실질적으로 이 사건 DB가 망분리 조치가 되었는가를 보아야하며, 이 사건 DB가 개인정보처리시스템에 포함되어 있지 않았는데도 단순히 피고 회사 내 부개발실과 외부망이 물리적으로 분리되었음을 이유로 망분리 조치를 다하였다고 보게 된다면 정보통신망법과 같은법 시행령 및 방통위고시의 기술적•관리적 보호조치 기준의 취지를 몰각하고 정보통신서비스 제공자등이 위 개인정보 보호를 위해 이행하여야할 의무를 피해갈 수 있는 길을 열어주는 것이라 할 것이기에 타당하지 않습니다.

비록 피고가 형식상의 기술적•관리적 보호조치 기준을 취하였다고 할지라도 이 사건 DB를 개인정보처리시스템에 포함시키지 않아서 이 사건 침해사고를 방지하지 못한 중대한 과실이 있기에 피고가 법률상 및 계약상 의무를 위반하였다고 봄이 타당합니다.

(3) 손해발생 여부

손해발생액에 대해서는 주위적 청구에서 본 바와 같습니다.

나. 예비적 청구 중 정보통신망법 제32조제1항 위반에 관하여

정보통신망법 제32조제1항은 정보통신서비스 제공자등이 이 장의 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자등에게 손해배상을 청구할 수 있다고 규정하는 바, 피고의 정보통신망법 위반 사항은 다음과 같습니다.

1) 정보통신망법 제23조(개인정보의 수집•제한 등) 위반에 관하여

(가) 정보통신서비스 제공자는 정보통신망법 제23제1항에 따라 사상, 신념, 가족 및 친인척 관계, 학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니되고, 설령 이용자의 동의를 받았다고 하더라도 같은 조 제2항에 따라 필요한 범위 내에서 최소한으로 위 개인정보를 수집하여야 합니다.

(나) 피고 회사 A가 운영하는 쇼핑몰 사이트 B는 오픈 마켓으로 개인 또는 소규모 업체 직접 상품을 등록하여 이를 판매하는 웹사이트인 바, 파악된 사실관계에 따르면 피고 회사 A는 원고들의 개인정보인 ID, 성별, 나이, 거주지 ('동'까지 기재) 이외에 최근 3개월간의 구매내역 (구매 일시, 구매한 물품명, 물품의 수량 및 가격, 제품 판매자, 상품평)을 수집하였습니다. 오픈 마켓의 운영을 위해 회원가입자 및 이용자들의 사용자 특정을 위한 ID, 그리고 배송 서비스 등의 중개를 위한 거주지의 정보 수집에 대해서는 필요최소한도 내의 수집이라 말할 수 있을 것이고 제23조제1항이 나열한 사생활을 뚜렷하게 침해할 우려가 있는 개인정보라고 볼 수는 없을 것이라 적법하다 할 것입니다.

그러나 그 이외 이용자들의 성별과 최근 3개월간의 구매내역 등이 수집된 점은 필요 최소한의 범위를 넘어선 개인정보 수집이라고 할 수 있습니다. 피고가 운영하는 오픈 마켓 형식의 운영 방식 특성상 B쇼핑몰의 회원가입자 및 이용자들의 3개월간 구매내역 등을 수집하는 것은 불필요한 것이라 할 것임에도 영리를 목적으로 한 빅데이터 분석을 위해 원고들이 B쇼핑몰에서 상품을 구매한 일지, 구매한 물품명, 물품의 수량 및 가격 등의 개인정보를 무단으로 수집하여 이를 별도로 이 사건 DB로 작성하였는바, 정보통신망법 제23조제2항에 따른 개인정보 최소수집의무를 위반하였다고 할 것입니다.

(다) 한편 원고 E는 위암 수술을 한 후 B 쇼핑몰 사이트를 통해서 "위암을 이겨낸 사람들", "위암 수술 후 식사 가이드", "암 치료 후 건강관리 가이드" 등의 서적을 구매하였고, 이러한 정보는 원고E의 병력(病歷)에 관한 것으로서 원고E의 사생활을 뚜렷하게 침해할 우려가 있는 개인정보에 해당함에도 피고는 이러한 점에 대한 고려 없이 이 사건 이 사건 DB를 작성하였으므로 피고는 정보통신망법 제23조제1항에 따른 개인정보 수집제한 규정을 명백히 위반하였다고 할 것입니다.

2) 정보통신망법 제25조 (개인정보의 취급위탁) 위반에 관하여

(가) 정보통신망법 제25조 제1항에 따르면 정보통신서비스 제공자는 제3자에게 이용자의 개인정보를 수집・보관・처리・이용・제공・관리・파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보 취급위탁"이라 한다)하는 경우에는 다음 각 호 (①개인정보 취급 위탁을 받는 자(이하 "수탁자", ②개인정보 취급위탁을 하는 업무의 내용)의 사항 모두를 이용자에게 알리고 동의를 받아야 합니다.

확인된 사실관계에 따르면 피고는 정보주체인 원고들로부터 개인정보를 제3자인 C회사에게 취급위탁한다는 사실에 대해서 위탁업무의 내용과 업무수탁자를 피고 홈페이지 개인정보처리방침에 공개하였을 뿐 해당 고객들로부터 위탁사실에 관한 동의를 전혀 얻은 바 없이 빅데이터 분석을 위한 이 사건 DB를 C에게 취급위탁한 잘못이 있습니다.

(나) 정보통신망법 제25조제4항은 정보통신서비스 제공자등은 수탁자가 이 장의 규정을 위반하지 아니하도록 관리•감독하여야 한다고 규정하고 있고, 같은 법 제25조제5항은 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자등의 소속직원으로 본다고 규정하고 있습니다.

피고는 빅데이터 분석 작업을 위해 C사와 위탁용역계약을 체결하였는바, , 피고는 C사에 대해서 C사가 정보통신망법 개인정보의 보호에 규정된 사항들을 위반하여 개인정보 누출이 없도록 관리•감독하여야할 의무가 있는데, 피고는 이러한 관리•감독의무를 다하지 못한 중대한 과실로 인해 이 사건 침해사고를 방지하지 못하였는바, 확인된 사실관계에 의하면 ① 피고는 C사와 위탁용역계약을 체결하면서 위탁용역계약서와 작업 투입인력에 대한 보안서약서를 작성하였지만 해당 문서 또는 별도의 계약으로 개인정보의 기술적•관리적 보호조치에 관한 사항 등 개인정보의 안전한 관리에 관한 특별한 약정을 하지 않았는바, 이는 피고가 정보통신망법 제25조제4항에 따라 C사가 정보통신망법 개인정보의 보호 관련 규정을 위반하지 않도록 하는 형식적인 관리•감독조차도 하지 않은 것이라고 보이고 ② 또한 피고는 위탁업무를 수행하는 C사의 직원들에게 프로젝트 시작 전 1회 보안교육을 시행하고 구체적으로 직원들의 업무를 감독하지 아니하였는데, 정보통신망법 제28조 및 같은 법 시행령에 따른 방통위고시 제3조제2항에 따르면 정보통신서비스 제공자등은 개인정보관리책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 실시하여야 하는바, 피고는 C사의 직원들을 대상으로 일회성의 보안교육을 시행하였을 뿐 C사 직원들의 업무와 관련하여 정기적인 교육 혹은 계속적으로 진행되는 업무에 대한 관리•감독을 하지 않았고 C사의 개인정보 관련 업무를 전임한 것으로 보입니다.

3) 정보통신망법 제27조의3 (개인정보 누출등의 통지•신고) 위반에 관하여

피고는 정보통신망법 제27조의3 제1항에 따라 "개인정보의 분실•도난•누출 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지•신고해서는 아니"되는 바, 사실관계에 의하면 피고는 2016. 7. 24 해킹사실을 알았음에도 불구하고 2016. 8. 1에 이르러서야 이를 이용자에게 통지하고 한국인터넷진흥원에

신고하여, 이 조항에서 규정한 통지•신고 의무를 위반하였습니다.

피고는 정확한 사실관계를 파악하기 위해서 법 제27조의3 제1항 본문의 정당한 사유에 해당한다고 항변할 것이나, 같은 법 시행령 제14조의2 제2항에 따르면 1. 누출등이 된 개인정보 항목, 2. 누출등이 발생한 시점에 대한 사항이 구체적으로 확인되지 아니한 경우라도 그 때까지 확인된 내용과 법 제27조의3 제1항제3호부터 제5호까지의 사항을 우선적으로 통지•신고하여야한다고 규정하고 있는바, 피고는 이러한 의무조차 이행하지 아니하였습니다.

4) 손해발생 여부

손해발생액에 대해서는 주위적 청구에서 본 바와 같습니다.

다. 정보통신망법 제32조의2에 따른 법정손해배상액 청구에 관하여

정보통신망법 제32조의2는 ①정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우, ②개인정보가 분실•도난•누출된 경우 제32조에 따른 손해배상을 청구하는 대신에 300만원 이하의 범위에서 상당한 금액을 손해배상액으로 청구할 수 있다고 합니다. 이에 대하여 ②에 대하여는 이미 증명된 사실관계가 있으므로 다툴 바가 없고, ①의 요건에 관하여는 앞에서의 주위적 청구와 예비적 청구의 검토에서 피고에게 과실이 있음을 증명하였습니다.

라. 피고의 제32조제1항 및 제32조의2의 "이 장의 위반"의 법리에 대한 항변

피고는 정보통신망법 제32조제1항 및 제32조의2의 요건으로서 "이 장의 위반"에 대해서 의무위반과 개인정보의 누출 사이에는 사실적 인과관계와 규범의 보호목적 관련성이 있어야 하며, 원고들이 주장하는 개인정보의 수집제한(제23조), 개인정보의 취급위탁(제25조), 개인정보 누출 등의 통지•신고(제27조의3) 등의 규정은 이 사건 침해와 이러한 관련성이 없기 때문에 제32조제1항 및 제32조의2의 요건으로서 "이 장의 위반"은 오로지 정보통신망법 제28조의 위반만이 해당된다고 주장할 것으로 보입니다.

그러나 위 정보통신망법상의 조문 중 다소 행정적 규제 목적으로 규정된 조항들도 있고 또한 개인정보의 분실・도난・누출과 긴밀한 직접적인 연관성이 다소 약하거나 희박한 것들도 있을지라도 신설된 제32조의2 법정손해배상 규정은 일반손해배상 규정인 정보통신망법 제32조 및 민법 제750조과 같이 전보적 성격을 지니고 있으므로 피고의 주장과 같이 주의의무의 근거가 되는 조문을 굳이 제한할 필요가 없다고 보입니다. 형식상으로도 정보통신망법 제32조의2 제1항은 정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우 및 개인정보가 분실・도난・누출된 경우를 모두 요구한다고 규정하면서 양자를 대등하게 규정하고 있으며 법정손해배상의 목적이 정보주체의 권리 구제 강화에 초점이 맞춰져 있을 뿐만 아니라, "이 장의 규정을 위반한" 것을 하나의 요건으로 설정한 것은 수집・보관・처리・이용・제공・관리・파기 등 개인정보의 전 생애주기에 걸쳐서 합법적인 처리를 담보하기 위한 것으로 보아야 하고, 이에 위반하여 개인정보가 불법적으로 처리되고 나아가

개인정보가 분실・도난・누출된 경우라면 법정손해배상을 인정할 수 있는 것으로 보아야 할 것이며 권리구제의 실질적 보장을 목적으로 하는 법정손해배상의 취지를 생각하건대 책임요건을 엄격히 제한하여 피고의 주장처럼 적용되는 조문을 제외하는 것은 타당하지 않는 것으로 보입니다.

마. 소결

피고는 이용계약상 채무불이행 및 정보통신망법 제23조, 제25조, 그리고 제27조의3의 규정을 위반하여 정보통신망법 제32조제1항의 손해배상책임을 지는바, 이를 대신하여 정보통신망법 제32조의2의 규정에 의거하여 원고들에게 각각 1,000,000원의 손해를 배상하도록 하는 판결을 구합니다.

3. 결론

주위적으로 피고는 원고들에게 각 3,000,000원 및 이에 대한 2016. 7. 23. 이 사건 소장 송달일까지는 연 5%의, 그 다음 날부터 다 갚는 날까지는 연 15%의 각 비율에 의한 금원을 각 지급하여야 하는 판결을, 예비적으로 피고는 원고들에게 각 1,000,000원 및 이에 대한 2016. 7. 23. 이 사건 소장 송달일까지는 연 5%의, 그 다음 날부터 다 갚는 날까지는 연 15%의 각 비율에 의한 금원을 각 지급하라는 판결을 구합니다.

2016. 9. 20.

위 원고 E, F, G 소송대리인 법무법인 정통,
담당변호사 정보호 (서명 또는 날인)

서울중앙지방법원 민사제22부 귀중