청 구 원 인

1. 당사자 관계

원고들은 피고와 이동통신 서비스 이용계약을 체결하고, 2025. 4. 18.경 별지목록 기재 휴대전화번호로 피고가 제공하는 이동통신 서비스를 이용하고 있었던 고객들입니다.[1)]

2. 이 사건 유심 정보 유출 사고의 발생 경위

가. 피고에 대한 사이버 공격 및 유심 정보 유출 발생

피고는 국내 최대 이동통신사업자로서 수많은 가입 고객들의 개인정보 및 통신 관련 중요 정보를 처리·보관하고 있는바, 이러한 정보의 안전한 관리에 대한 고도의 주의의무를 부담하고 있습니다.

그럼에도 불구하고, 피고는 2025. 4. 18.경 (또는 그 이전부터 지속된 것으로 추정되는) 외부 해커로부터 사이버 공격(공격에 사용된 악성코드는 'BPFDoor' 계열 등으로 추정됩니다)을 받아, 피고가 운영·관리하던 핵심 서버 시스템에 대한 불법적인 접근 및 침투를 허용하였습니다.

그 결과, 피고가 관리하던 이동통신 가입 고객들, 즉 원고들을 포함한 다수 피해자들의 유심(USIM, Universal Subscriber Identity Module) 및 이와 관련된 극히

1) 갑 제1호증, 별지목록

민감한 개인정보가 외부로 대량 유출되는 중대한 보안 사고(이하 '이 사건 사고'라고 합니다)를 당하게 되었습니다. 이 사건 사고는 단순한 서비스 장애를 넘어, 가입자들의 통신 비밀과 개인정보 자기결정권에 대한 심각한 침해를 야기한 것입니다.

나. 과학기술정보통신부 1, 2차 조사결과를 통해 확인된 유출 정보의 심각성

이 사건 사고의 심각성은 정부 당국의 조사결과 발표를 통해 더욱 명확하게 드러났습니다. 과학기술정보통신부(이하 '과기정통부')는 민관합동조사단을 구성하여 이 사건 사고에 대한 조사를 진행하였고, 2025. 4. 29.자 1차 조사결과 발표에 이어, 2025. 5. 19.자 2차 조사결과 발표를 통해 유출된 정보의 구체적인 내용과 규모, 그리고 그로 인한 잠재적 위험성을 공식적으로 확인하였습니다.[2)]

1) 유출 정보의 종류 및 규모 (IMSI, ICCID, IMEI, 데이터 총량 등)

과기정통부 조사결과 등에 따르면, 이 사건 사고로 유출된 정보에는 가입자들의 휴대전화번호는 물론, 가입자식별번호(IMSI, International Mobile Subscriber Identity) 약 2,695만 7,749건, 유심카드 고유 일련번호(ICCID, Integrated Circuit Card Identifier)가 포함되어 있음이 확인되었습니다. 더욱이, 당초 피고 및 정부가 유출 가능성을 부인했던 단말기 고유식별번호(IMEI, International Mobile Equipment Identity) 역시 약 29만 1,831건이 유출된 사실이 2차 조사결과를 통해 새롭게 밝혀졌습니다. 이처럼 유출된 데이터의 총량은 최소 9.82GB에 달하는 막

2) 갑 제2호증, 과학기술정보통신부 1차 보도자료, 갑 제3호증, 과학기술정보통신부 2차 보도자료

대한 규모로, 이는 피고가 보유한 고객 정보가 광범위하게 외부로 노출되었음을 의미합니다.

2) ‘유심 비밀키(K)’ 등 절대적 인증 정보 유출 가능성 및 그 위험성

특히 심각한 점은, 유심 복제(SIM Cloning) 및 이를 통한 2차 범죄에 직접적으로 악용될 수 있는 핵심 정보들이 유출되었다는 사실입니다. 과기정통부 조사결과에서도 명시되었듯이, IMSI, ICCID, IMEI 등은 유심 복제의 핵심 요소가 될 수 있는 매우 민감한 정보입니다. 나아가, 통신사와 유심 간의 상호 인증 및 통신 암호화에 사용되는 ‘유심 인증키(Ki)’ 또는 ‘유심 비밀키(K)’와 같은 절대적인 인증 정보까지 유출되었을 가능성이 강력하게 제기되고 있습니다. 만약 이러한 절대적 인증 정보까지 해커의 손에 넘어갔다면, 이는 단순한 개인정보 유출을 훨씬 뛰어넘어, 피해자들의 통신 수단이 완전히 타인에게 장악될 수 있음을 의미합니다. 이는 곧 명의 도용을 통한 대포폰 개통, 금융 계좌 부정 개설 및 자금 탈취, 스미싱 및 보이스피싱 등 각종 금융사기, 사생활 침해 등 상상하기 어려운 수준의 직접적이고 회복 불가능한 2차 피해로 이어질 수 있는 중대한 위험 요소입니다. 이는 사실상 피해자들의 ‘디지털 신분증’과 ‘인감도장’이 통째로 탈취당한 것과 다름없는 심각한 상황이라 할 것입니다.

3. 피고의 의무 위반 및 과실

정보주체는 개인정보처리자가 개인정보보호법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있습니다(개인정보보호법 제39조 제1

항). 피고는 국내 최대 이동통신사업자이자 방대한 규모의 개인정보를 처리하는 개인정보처리자로서, 개인정보보호법 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법') 등 관련 법령에 따라 개인정보의 안전한 관리를 위한 각종 기술적·관리적 보호조치를 철저히 이행하여야 할 포괄적이고 중대한 법적 의무를 부담합니다. 그러나 피고는 다음과 같이 개인정보보호법상 중대한 의무들을 명백히 위반하였습니다.

가. 개인정보보호법 관련 의무 위반

1) 개인정보의 안전성 확보조치 의무 위반 (개인정보보호법 제29조)

개인정보보호법 제29조는 개인정보처리자에게 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획의 수립, 접속기록의 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 할 의무를 부과하고 있습니다. 또한, 동법 시행령 제30조 및 개인정보보호위원회 고시 「개인정보의 안전성 확보조치 기준」은 이러한 보호조치의 구체적인 내용을 정하고 있습니다.

그러나 이 사건 사고의 발생 경위, 특히 앞서 살펴본 바와 같이 ① 피고의 핵심 서버들이 약 3년이라는 장기간 동안 악성코드에 감염된 채 방치되었던 점, ② 최소 23대에 달하는 서버가 감염되고 25종에 이르는 다양한 악성코드가 발견된 점, ③ 가입자식별번호(IMSI), 유심카드 일련번호(ICCID)는 물론, 단말기 고유식별번호(IMEI)와 같은 극도로 민감한 정보가 대량 유출되었고, 심지어 '유심 비밀키(K)'

의 유출 가능성까지 제기된 점 등은 피고가 다음과 같은 구체적인 안전성 확보조치 의무를 현저히 해태하였음을 명백히 보여줍니다.

가) 내부 관리계획 수립·시행 미흡

피고는 개인정보의 안전한 처리를 위한 내부 관리계획을 수립하고 이를 지속적으로 시행·점검해야 함에도 불구하고, 장기간의 보안 취약점 방치 등은 내부 관리계획이 형식적으로 운영되었거나 그 실효성이 매우 낮았음을 시사합니다.

나) 접근 통제 및 접근 권한 관리 소홀

피고는 가입자 인증 정보 등 민감 정보가 저장된 핵심 서버(HSS 등)에 대한 접근 통제 시스템을 제대로 구축·운영하지 아니하고, 비인가 접근 시도를 적절히 차단하지 못하는 등 보안 관리를 현저히 소홀히 하여 해커의 침투 및 정보 유출을 허용한 것으로 보입니다.

피고는 개인정보처리시스템에 대한 접근 권한을 최소한의 인원에게만 부여하고, 권한 변경·말소에 대한 기록을 남기고 관리해야 함에도, 이러한 접근 권한 관리를 부실하게 하여 불필요한 권한이 부여되거나 퇴직자 등의 접근 권한이 즉시 말소되지 않는 등의 문제가 있었을 가능성이 높습니다.

다) 개인정보의 암호화 조치 미흡

피고는 법령에 따라 고유식별정보, 비밀번호, 바이오정보 등 주요 개인정보를 안전한 알고리즘으로 암호화하여 저장·전송해야 함에도 불구하고, 이 사건에서

유출된 IMSI, ICCID, IMEI 등의 정보에 대한 암호화 조치가 미흡했거나, 해커가 쉽게 해독할 수 있는 취약한 방식으로 암호화했을 가능성이 제기됩니다.

특히, 통신 암호화 및 인증의 핵심인 '유심 비밀키(K)'와 같은 절대적 인증 정보에 대해서는 더욱 강력한 암호화 및 접근 통제 조치가 요구됨에도, 피고는 이러한 핵심 인증 정보의 암호화 조치를 소홀히 하였거나 아예 적용하지 않았을 가능성마저 배제할 수 없습니다.

라) 접속기록의 보관 및 위조·변조 방지를 위한 조치 미흡

피고는 개인정보처리시스템에 접속한 기록을 최소 1년 이상(개인정보보호위원회 고시 기준에 따라서는 2년 이상) 보관·관리해야 함에도, 약 3년간 악성코드에 감염된 정황은 이러한 접속기록 보관 의무가 제대로 이행되지 않았거나, 기록이 있더라도 분석 및 대응에 활용되지 못했음을 시사합니다.

피고는 접속기록이 위·변조되거나 도난, 분실되지 않도록 안전하게 보관해야 함에도, 2022. 6. 15.부터 2024. 12. 2.까지의 기간에 대한 로그 기록이 존재하지 않는 등 접속기록 관리의 허점을 드러냈습니다.

마) 보안프로그램의 설치 및 운영 미흡

피고는 개인정보처리시스템 및 개인정보취급자의 컴퓨터 등에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영해야 함에도, 25종에 이르는 다양한 악성코드가 발견된 사실은 이러한 보안 프로그

램이 제 기능을 하지 못했거나 부실하게 운영되었음을 의미합니다.

피고는 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일일 1회 이상 업데이트를 실시하여 최신 상태로 유지해야 함에도, 이를 소홀히 하여 신종 악성코드에 대한 방어에 실패한 것으로 보입니다.

바) 침입 탐지 및 차단 시스템 부실 운영

피고는 외부로부터의 불법적인 침입 시도를 실시간으로 탐지하고 차단할 수 있는 침입차단시스템 및 침입탐지시스템을 설치·운영해야 함에도, 최소 23대의 서버가 장기간 악성코드에 감염된 사실조차 인지하지 못한 점은 해당 시스템이 부실하게 운영되었거나, 탐지된 이상 징후에 대한 적절한 대응이 이루어지지 않았음을 강력히 시사합니다.

사) 소결

이러한 피고의 다층적이고 총체적인 안전성 확보조치 의무 위반은 개인정보보호 관련 법령 및 고시에서 정한 구체적인 기술적·관리적 보호조치 수준에 현저히 미달하는 명백하고 중대한 과실에 해당하며, 이로 인해 이 사건 정보 유출 사고가 발생하였다고 할 것입니다.

2) 개인정보 유출 등의 통지·신고 의무 위반 (개인정보보호법 제34조)

개인정보보호법 제34조 제1항은 개인정보처리자가 개인정보의 유출등(분실·도난·유출·위조·변조 또는 훼손)을 알게 되었을 때에는 '지체 없이' 해당 정

보주체에게 유출된 개인정보의 항목, 유출된 시점과 그 경위 등을 통지하여야 한다고 규정하고 있으며, 같은 조 제3항 및 동법 시행령 제39조는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우 개인정보보호위원회 또는 대통령령으로 정하는 전문기관(한국인터넷진흥원 등)에 '지체 없이'(72시간 이내) 신고하도록 규정하고 있습니다.

그럼에도 피고는 이 사건 사고 발생을 2025. 4. 19.경 최초 내부 인지하였음에도 불구하고, 원고들을 포함한 정보주체들에게는 그로부터 무려 20일 이상이 경과한 2025. 5. 9.에 이르러서야 비로소 유심 관련 개인정보 유출 가능성에 대한 형식적인 통지를 하였을 뿐입니다.[3] 해당 통지에는 유출된 개인정보의 구체적인 항목(특히 IMEI 유출 사실 누락)이나 피해를 최소화하기 위한 정보주체의 구체적인 방법 등에 대한 상세한 설명이 부족하였습니다. 또한, 개인정보보호위원회 또는 한국인터넷진흥원에 대한 신고 역시 사고 인지 후 3일(또는 언론 보도에 따르면 45시간 이상)이 지난 2025. 4. 22.경에야 이루어진 것으로 알려져, 법에서 정한 '지체 없는' 통지 및 신고 의무를 명백히 위반하였습니다. 특히, IMEI 유출과 같이 피해자들의 불안감을 증폭시킬 수 있는 중대한 사실에 대해서는 초기에 정보를 은폐하려 한 정황까지 드러나, 피고의 통지 및 신고 의무 위반은 더욱 비난받아 마땅합니다. 이러한 지연되고 불충분하며 기만적이기까지 한 통지 및 신고는 정보주체인 원고들이 사고 발생 사실을 신속히 인지하고 2차 피해 방지를 위한 적절한 대응 조치를 취할 수 있는 골든타임을 놓치게 하였으며, 피해 확산 방지를 위한 관계 기관의 즉각적인 조사 및 기술 지원 기회를 박탈한 중대한 과실에 해

3) 갑 제4호증, 피고 발송 문자메시지

당합니다.

3) 개인정보 유출 등에 따른 피해 최소화를 위한 대책 마련 및 필요한 조치 의무 위반 (개인정보보호법 제34조 제2항)

개인정보보호법 제34조 제2항은 개인정보처리자에게 개인정보 유출등이 발생한 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 할 의무를 부과하고 있습니다.

그러나 이 사건 사고 발생 이후 피고의 대응은 전반적으로 혼란스럽고 미흡하기 짝이 없었습니다. IMEI 유출 사실을 뒤늦게 인정하며 피해자들의 불안감을 가중시킨 점, 유심 교체 과정에서 발생한 피해자들의 시간적·경제적 부담에 대한 실질적인 지원책이 부족했던 점, 2차 피해에 대한 불안감을 해소하기 위한 구체적이고 적극적인 조치가 미흡했던 점 등을 고려하면, 피고가 사전에 적절한 대응 매뉴얼을 구비하고 있었는지, 그리고 이에 따라 사고 원인 제거 및 재발 방지 조치를 충분히 이행했는지, 나아가 정보주체의 불편과 경제적 부담을 최소화하기 위한 진정성 있는 노력을 다했는지에 대해 심각한 의문을 제기하지 않을 수 없습니다. 이는 피고가 피해 최소화를 위한 대책 마련 및 조치 의무를 제대로 이행하지 아니한 중대한 과실에 해당합니다.

4) 고의·과실에 대한 입증책임 전환 (개인정보보호법 제39조 제1항 제2문)

개인정보보호법 제39조 제1항 제2문은 “개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 정보주체에게 발생한 손해를 배상할 책임을 면할 수

없다.” 라고 규정하여, 개인정보 유출로 인한 손해배상책임에 있어 입증책임을 개인정보처리자에게 전환하고 있습니다.

앞서 상세히 살펴본 바와 같이, 이 사건 유심 정보 유출 사고의 발생 경위, 즉 장기간의 악성코드 감염 방치, 다수의 서버 감염, IMEI를 포함한 극도로 민감한 정보의 대량 유출, 피고의 안일하고 기만적이기까지 한 사후 대응 과정 등을 종합적으로 고려할 때, 피고의 중대한 과실은 명백히 추정됩니다. 따라서 피고는 이 사건 사고 발생 및 그로 인한 원고들의 손해 발생에 있어 자신에게 고의 또는 과실이 없음을 적극적으로 입증하지 못하는 한, 원고들이 입은 손해에 대하여 배상할 책임을 면할 수 없습니다.

나. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (정보통신망법) 관련 의무 위반

피고는 정보통신서비스 제공자로서 개인정보보호법뿐만 아니라 정보통신망법상 규정된 정보보호 관련 의무 또한 철저히 준수해야 합니다. 그러나 피고는 다음과 같이 정보통신망법상 중대한 의무들을 위반하였습니다.

1) 정보통신망의 안정성 확보 등을 위한 보호조치 의무 위반 (정보통신망법 제45조)

정보통신망법 제45조 제1항은 정보통신서비스 제공자 등이 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다고 규정하고 있으며, 같은 조 제2항은 과학기술정보통신부장관이

이러한 보호조치의 구체적인 내용을 정한 ‘정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시’(또는 관련 ‘정보보호지침’)를 정하여 준수하도록 권고할 수 있다고 규정하고 있습니다.

앞서 개인정보보호법 위반 항목에서 상세히 지적한 바와 같이, 피고는 ① 핵심 서버에 대한 접근 통제 및 보안 관리 소홀, ② 침입 탐지 및 차단 시스템의 부실 운영, ③ 핵심 정보에 대한 암호화 조치 미흡, ④ 악성코드 감염에 대비한 충분한 보안 대책 미비 등 정보보호지침에서 정한 기술적·관리적 보호조치 수준에 현저히 미달하는 방식으로 정보보호 의무를 이행하지 못하였습니다.

가) 관리적 보호조치 미흡

피고는 정보보호 정책 및 정보보호 조직을 적절히 수립·운영하고, 정보보호 교육을 실시하며, 정기적인 위험 분석 및 관리를 통해 정보보호 대책을 수립·시행해야 함에도, 장기간의 보안 취약점 방치 및 다수 서버의 악성코드 감염 사실은 이러한 관리적 보호조치가 극히 부실했음을 보여줍니다.

나) 기술적 보호조치 미흡

피고는 접근 통제, 암호화, 악성코드 방지, 침입차단시스템 및 침입탐지시스템 운영, 접속기록 관리 등 핵심적인 기술적 보호조치를 소홀히 하여 이 사건 정보 유출 사고를 야기하였습니다. 특히, 25종의 악성코드 발견 및 약 3년간의 감염 방치는 기술적 보호조치의 총체적 부실을 의미합니다.

다) 소결

이러한 정보보호지침 미준수는 정보통신망의 안정성 및 정보의 신뢰성 확보라는 입법 취지를 정면으로 위배하는 것으로, 피고의 중대한 과실에 해당합니다.

2) 침해사고의 신고 의무 위반 (정보통신망법 제48조의3)

정보통신망법 제48조의3 제1항은 정보통신서비스 제공자가 침해사고가 발생하면 '즉시'(대통령령으로 정하는 바에 따라 24시간 이내) 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원(KISA)에 신고하여야 한다고 규정하고 있습니다. 이는 신속한 사고 대응 및 피해 확산 방지를 위한 핵심적인 의무입니다.

그러나 피고는 2025. 4. 19.경 이 사건 사고를 최초 인지하였음에도 불구하고, 관계 기관에는 3일이 지난 2025. 4. 22.경에야 신고한 것으로 알려져,[4] 위 신고 의무를 명백히 위반하였습니다. 이러한 신고 지연은 사고 발생 초기에 신속한 대응과 피해 확산 방지를 위한 골든타임을 놓치게 하고, 관계 기관의 즉각적인 조사 및 기술 지원 기회를 박탈한 중대한 과실에 해당합니다.

3) 침해사고의 원인 분석 및 피해 확산 방지 조치 의무 소홀 (정보통신망법 제48조의4)

정보통신망법 제48조의4 제1항은 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 그 결과에 따라 피

4) 갑 제5호증, 관련 연합뉴스 보도자료

해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다고 규정하고 있습니다. 이 사건 사고와 같이 가입자의 통신 비밀 및 금융 거래 안전과 직결되는 IMEI를 포함한 유심 정보가 대규모로 유출된 사안은 '중대한 침해사고'에 해당하며, 피고는 침해사고의 정확한 원인을 신속하고 철저하게 분석하고, 그 결과를 바탕으로 피해 확산을 막기 위한 효과적인 기술적·관리적 조치를 즉각적으로 시행했어야 합니다.

그러나 ① 약 3년간의 악성코드 감염 방치, ② 최소 23대의 서버 감염 및 25종의 악성코드 발견, ③ IMEI 유출 사실 은폐 시도 및 로그 기록 부재로 인한 추가 유출 가능성 방치 등은 피고의 내부적인 원인 분석, 피해 확산 방지 조치 및 사후 대응이 극히 미흡했거나 적절한 시기에 이루어지지 않았음을 강력히 시사합니다. 이는 피고가 침해사고 대응 및 원인 분석 관련 의무를 소홀히 한 중대한 과실입니다.

4) 주요정보통신서비스 제공자로서의 이용자 정보보호 조치 의무 미흡 (정보통신망법 제47조의4)

정보통신망법 제47조의4 제3항은 피고와 같은 '주요정보통신서비스 제공자'에게 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있도록 규정하고 있습니다.

이 사건 사고 후 원고들을 포함한 이용자들은 피고의 안내에 따라 유심을 교체하는 등 사실상의 보호조치를 취해야 했으며, 일부 금융기관 등에서는 피고의 이동통신 서비스를 이용하는 고객에 대한 SMS 본인 인증을 일시 중단하거나 강화하는 등의 조치가 이루어져 금융 거래나 온라인 서비스 이용 시 추가적인 불편과 제약을 감수해야 했습니다. 이는 피고가 이용자 보호조치를 안내하고 이행을 요구하는 과정에서 ① 그 내용과 절차의 적절성, ② 이용약관에 따른 명확한 근거 제시, ③ 이용자 불편 최소화를 위한 충분한 지원 제공 등의 의무를 다하였는지에 대한 심각한 의문을 제기합니다. 특히, IMEI 유출 가능성을 초기에 부인하다가 뒤늦게 번복한 점, 유심 교체를 강제가 아닌 권고 수준으로 안내하며 책임을 회피하려는 듯한 태도를 보인 점, 위약금 면제에 대한 소극적인 자세 등은 피고의 조치가 형식적인 안내에 그치거나 이용자에게 일방적으로 부담을 전가하는 방식으로 이루어졌을 가능성을 높이며, 이는 동 조항의 취지에 명백히 반하는 것입니다.

5) 정보보호 최고책임자(CISO) 지정 및 업무 총괄 책임 방기 (정보통신망법 제45조의3)

정보통신망법 제45조의3 제1항은 정보통신서비스 제공자가 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다고 규정하고 있으며, 같은 조 제4항은 정보보호 최고책임자가 정보보호 계획의 수립·시행 및 개선, 정보보호 실태와 관행의 정기적인 감사 및 개선, 정보보호 위험의 식별 평가 및 정보보호 대책 마련 등의 업무를 총괄하도록

규정하고 있습니다.

이 사건 유심 정보 유출 사고는 국가의 핵심 통신 인프라를 담당하는 피고에게서 발생한 것으로서, 그 유출된 정보의 민감성과 잠재적 피해 규모는 가늠하기 어려울 정도로 막대합니다. 이는 곧 피고의 정보보호 최고책임자가 법률상 부여된 핵심적인 정보보호 업무, 특히 시스템 취약점 관리, 침해사고 예방 및 효과적인 대응체계 구축·운영이라는 중대한 책무를 제대로 이행하지 못했음을 반증하는 것입니다. 장기간의 악성코드 감염 방치, 다수의 서버 감염, 핵심 정보 유출 등은 피고의 정보보호 거버넌스 및 관리 시스템에 총체적인 부실이 있었음을 명백히 나타냅니다. 고학수 개인정보보호위원회 위원장 또한 2025. 4. 28. 국회 정무위원회 전체회의에서 이번 사고가 “과거 LG유플러스나 KT (유출) 사건에 비해서도 훨씬 더 중대한 상황“이며, 강화된 법 규정에 따라 피고에게 “상당한 수준의 처벌 가능성“이 있다고 언급한 바 있습니다. 이는 CISO의 업무 총괄 책임이 제대로 이행되지 않았음을 뒷받침하는 정황입니다.

4. 원고들의 손해 발생 (정신적 고통)

원고들은 피고의 중대한 과실로 인하여 발생한 이 사건 사고로 말미암아, 개인정보 자기결정권 및 사생활의 비밀과 자유를 심각하게 침해당하였을 뿐만 아니라, 그로 인한 직접적이고 극심한 정신적 고통을 겪고 있습니다.

가. IMEI 및 유심 비밀키(K) 등 절대적 인증 정보 유출 가능성으로 인한 극심한 정신적 고통

원고들이 겪는 정신적 고통의 핵심적인 원인은 단순한 개인정보의 유출을 넘어, 통신 및 금융 거래의 핵심 인증 수단인 유심(USIM) 정보, 특히 단말기 고유식별번호(IMEI)가 실제로 유출되었고, 나아가 유심 인증키(Ki) 또는 '유심 비밀키(K)'와 같은 절대적인 인증 정보까지 외부에 유출되었을 가능성이 매우 높다는 사실 그 자체에 있습니다.

IMEI는 스마트폰의 주민등록번호와 같은 역할을 하며, 이것이 다른 개인정보와 결합될 경우 특정 개인을 표적으로 한 정교한 공격에 악용될 수 있습니다. 더욱이, 만약 통신사와 유심 간의 암호화된 통신 및 인증에 사용되는 '유심 비밀키(K)'까지 유출되었다면, 이는 원고들의 스마트폰 자체가 사실상 해커에게 복제되거나 통제될 수 있는 '디지털 신분증 탈취' 또는 '디지털 인감 도용'과 다름없는 극히 위험한 상황을 의미합니다.

원고들은 이러한 절대적 인증 정보의 유출 가능성으로 인해, ① 자신의 명의가 도용되어 불법적인 대포폰이 개통되거나, ② 자신도 모르는 사이에 금융 계좌가 개설되어 거액의 대출이 실행되거나 자금이 인출되는 등의 금융사고가 발생할 수 있다는 점, ③ 자신의 스마트폰을 통해 발송되는 문자나 통화 내용이 감청되거나 조작될 수 있다는 점, ④ 나아가 자신의 사생활이 송두리째 노출되거나 감시당할 수 있다는 점 등 상상할 수 있는 최악의 시나리오들에 대한 극심한 불안감과 공포심을 일상적으로 느끼고 있습니다. 이는 단순한 우려를 넘어, 자신의 신원과 재산, 사생활 전체가 언제든 침해될 수 있다는 실존적인 위협감으로 다가오고 있으며, 이로 인해 원고들은 잠 못 이루는 밤을 보내는 등 심각한 정신적 스트레스에

시달리고 있습니다.

나. 2차 피해(명의도용, 금융사기 등)에 대한 현실적인 공포감 및 불안감

이 사건 사고로 유출된 가입자식별번호(IMSI), 유심카드 일련번호(ICCID), 단말기 고유식별번호(IMEI) 및 유출 가능성이 높은 '유심 비밀키(K)' 등은 단순한 개인 식별 정보를 넘어, 유심 복제(SIM Cloning)를 통한 각종 2차 범죄에 직접적으로 악용될 수 있는 핵심적인 수단입니다. 원고들은 이러한 정보가 이미 해커의 손에 넘어갔거나 불법적인 경로를 통해 유통될 수 있다는 사실만으로도 언제든지 다음과 같은 심각한 2차 피해의 대상이 될 수 있다는 현실적인 공포감과 지속적인 불안감에 시달리고 있습니다.

첫째, 명의 도용을 통한 불법 대포폰 개통 및 범죄 악용의 위험입니다. 유출된 정보를 이용하여 원고들 모르게 원고들의 명의로 대포폰이 개통되고, 이것이 보이스피싱, 스미싱, 불법 도박 등 각종 범죄에 사용될 경우, 원고들은 자신도 모르는 사이에 범죄에 연루되거나 그로 인한 법적·경제적 책임을 부당하게 추궁당할 수 있다는 극심한 불안감을 느끼고 있습니다.

둘째, 금융 계좌 부정 개설, 대출 실행, 자금 탈취 등 직접적인 금융 사기의 위험입니다. 해커가 유심 복제 등을 통해 원고들의 금융 접근 권한을 탈취하여, 원고들 명의로 새로운 금융 계좌를 개설하고 이를 통해 불법적인 자금 이동 통로로 사용하거나, 원고들 모르게 거액의 대출을 실행하여 막대한 금전적 피해를 입힐 수 있다는 공포에 시달리고 있습니다. 또한, 기존 계좌에서 자금이 무단으로 인출

되거나, 고액의 상품이 자신도 모르게 결제되는 등의 피해가 발생할 수 있다는 불안감 역시 원고들의 일상을 짓누르고 있습니다. 최근 유명인의 유심 복제를 통해 수십억 원대의 가상자산이 탈취된 사건 등은 이러한 우려가 결코 기우가 아님을 명백히 보여주는 사례입니다.

셋째, 스미싱, 보이스피싱 등 정교화된 전자금융사기의 표적이 될 위험입니다. 유출된 IMEI와 전화번호 등은 해커로 하여금 특정 개인을 대상으로 한 맞춤형 스미싱 문자나 보이스피싱 시나리오를 구성하는 데 악용될 수 있습니다. 원고들은 자신이 이러한 정교한 사기 범죄의 표적이 되어 심리적으로 기만당하고 금전적 피해를 입을 수 있다는 끊임없는 불안감 속에서 생활하고 있습니다.

이처럼 원고들은 이 사건 사고로 인해 자신의 신원과 재산이 언제든 범죄의 도구로 사용되거나 직접적인 피해의 대상이 될 수 있다는 구체적이고 현실적인 공포감에 휩싸여 있으며, 이는 일상생활 전반에 걸쳐 심각한 불안과 스트레스를 야기하고 있습니다.

다. 평온한 일상생활의 심각한 방해

이 사건 사고로 인한 지속적인 불안감과 2차 피해에 대한 공포는 원고들의 평온했던 일상생활을 심각하게 방해하고 있습니다. 이전에는 아무런 의심 없이 사용했던 스마트폰과 온라인 서비스가 이제는 잠재적인 위험 요소로 인식되면서, 원고들은 다음과 같은 일상생활의 불편과 제약을 감수하며 살아가고 있습니다.

첫째, 금융 거래 및 온라인 서비스 이용 시 과도한 경계와 확인 절차 반복입니

다. 원고들은 자신의 금융 계좌에서 비정상적인 거래가 발생하지 않았는지 수시로 확인해야 하는 강박관념에 시달리고 있으며, 인터넷뱅킹이나 모바일 결제 시 이전보다 훨씬 더 많은 시간을 할애하여 보안 상태를 점검하고 인증 절차를 반복하는 등 극도의 경계심을 늦추지 못하고 있습니다. 이는 일상적인 경제활동에 상당한 피로감과 스트레스를 더하고 있습니다.

둘째, 의심스러운 문자나 전화에 대한 극도의 민감성과 불필요한 시간 소모입니다. 원고들은 출처가 불분명한 문자메시지나 전화에 대해서는 혹시 모를 스미싱이나 보이스피싱일 수 있다는 생각에 극도로 민감하게 반응하게 되었으며, 이를 확인하고 대처하는 데 불필요한 시간과 감정을 소모하고 있습니다. 심지어 정상적인 안내 문자나 필요한 연락조차 의심하게 되어 원활한 소통에 어려움을 겪는 경우도 발생하고 있습니다.

셋째, 스마트폰 사용 자체에 대한 불안감과 자기 검열 심화입니다. 스마트폰이 개인정보 유출의 통로이자 범죄의 매개체가 될 수 있다는 인식은 원고들로 하여금 스마트폰 사용 자체에 대한 막연한 불안감을 느끼게 만들고 있습니다. 개인적인 정보가 담긴 사진이나 메시지, 금융 정보 등을 스마트폰에 저장하거나 전송하는 행위 하나하나에 대해 이전보다 훨씬 더 많은 자기 검열을 하게 되었으며, 이는 자유로운 정보 활용과 소통을 위축시키는 결과를 초래하고 있습니다.

넷째, 정신적 피로감 누적 및 대인 관계 위축 가능성입니다. 지속적인 불안과 긴장 상태는 원고들의 정신적 피로감을 누적시키고 있으며, 이는 수면 장애, 집중력 저하 등 다양한 신체적·정신적 증상으로 이어질 수 있습니다. 또한, 타인에게

자신의 개인정보가 유출되었을 수 있다는 불안감은 대인 관계에 있어서도 소극적인 태도를 유발하거나 불필요한 오해를 낳을 수 있는 등 사회생활 전반에 부정적인 영향을 미치고 있습니다.

이처럼 원고들은 이 사건 사고로 인해 이전에는 당연하게 누려왔던 일상생활의 평온함과 자유로움을 심각하게 침해당하였으며, 이는 정신적 고통을 가중시키는 중요한 요인이 되고 있습니다.

라. 피고의 미흡한 사후 대응으로 인한 정신적 고통 가중

이 사건 사고 발생 이후, 원고들은 피고의 책임 있는 자세와 신속하고 적절한 피해 구제 조치를 기대하였으나, 피고는 오히려 미흡하고 안일하며 심지어 기만적이기까지 한 사후 대응으로 일관하여 원고들의 정신적 고통을 더욱 가중시켰습니다.

첫째, 사고 발생 사실 및 유출 정보 범위에 대한 늑장·부실 고지 및 정보 은폐 시도입니다. 피고는 사고 인지 후 20일 이상이 지나서야 피해자들에게 형식적인 유출 가능성 통지를 하였을 뿐만 아니라, 특히 피해 규모와 심각성을 가늠할 수 있는 핵심 정보인 단말기 고유식별번호(IMEI) 유출 사실에 대해서는 초기에 부인하다가 정부의 2차 조사결과 발표 이후에야 마지못해 인정하는 등 정보를 은폐·축소하려는 듯한 태도를 보였습니다. 이는 피해 사실을 정확히 파악하고 신속하게 대처해야 할 원고들의 권리를 침해하고, 피고에 대한 불신과 분노를 극대화시켜 정신적 고통을 심화시켰습니다.

둘째, 유심 교체 등 피해 방지 조치에 대한 소극적 안내와 책임 회피적 태도입니다. IMEI 및 유심 비밀키(K) 유출 가능성이 제기된 심각한 상황임에도 불구하고, 피고는 유심 교체를 강력히 권고하고 그 과정에서의 불편과 비용을 적극적으로 지원하기보다는, 형식적인 안내에 그치거나 마치 피해자들의 선택 사항인 것처럼 책임을 회피하려는 듯한 인상을 주었습니다. 이로 인해 원고들은 유심 교체의 필요성과 시급성에 대해 혼란을 겪었으며, 스스로 시간과 비용을 들여 유심을 교체하는 과정에서 상당한 불편과 경제적 부담을 감수해야 했습니다. 이러한 피고의 무책임한 태도는 피해자들의 불안감을 방치하고 정신적 고통을 가중시킨 요인이 되었습니다.

이처럼 피고의 사고 발생 이후 보여준 일련의 미흡하고 무책임한 사후 대응은, 이미 이 사건 사고 자체로 극심한 정신적 고통을 겪고 있는 원고들에게 피해자로서 존중받지 못하고 있다는 무력감과 분노를 더하여 그 정신적 고통을 배가시켰습니다.

마. 개인정보 자기결정권 및 사생활의 비밀과 자유 침해

이 사건 사고 및 그로 인한 피고의 제반 의무 위반 행위는 원고들의 헌법상 기본권인 개인정보 자기결정권 및 사생활의 비밀과 자유를 중대하게 침해하는 결과를 초래하였습니다.

첫째, 개인정보 자기결정권의 본질적 침해입니다. 개인정보 자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지

를 정보주체 스스로가 결정할 수 있는 권리입니다. 그러나 이 사건 사고로 인해 원고들의 휴대전화번호, 가입자식별번호(IMSI), 유심카드 일련번호(ICCID), 단말기 고유식별번호(IMEI) 등 민감한 개인정보가 원고들의 의사와는 전혀 무관하게 불법적으로 유출되었고, 심지어 '유심 비밀키(K)'와 같은 절대적 인증 정보까지 유출되었을 가능성이 제기됨으로써, 원고들은 자신의 개인정보에 대한 통제권을 상실하였습니다. 이는 원고들이 자신의 개인정보를 보호하고 스스로 관리할 수 있는 권리를 근본적으로 침해당한 것입니다.

둘째, 사생활의 비밀과 자유의 심각한 위협입니다. 유출된 정보, 특히 IMEI와 유심 비밀키(K) 등의 정보는 원고들의 통신 내용, 위치 정보, 온라인 활동 등 사생활의 핵심적인 영역을 타인이 들여다보거나 감시할 수 있는 수단으로 악용될 가능성을 내포하고 있습니다. 원고들은 자신의 가장 사적인 영역이 언제든 침해될 수 있다는 불안감 속에서 생활해야 하며, 이는 자유로운 의사 표현이나 행동을 위축시키고 사생활의 평온을 심각하게 저해하는 결과를 가져옵니다. 이처럼 자신의 사생활이 타인에게 노출되거나 감시당할 수 있다는 불안감은 그 자체로 사생활의 비밀과 자유에 대한 중대한 침해에 해당합니다.

셋째, 신뢰 관계의 파괴 및 정신적 안녕의 침해입니다. 원고들은 피고가 국내 최대 이동통신사업자로서 자신의 개인정보를 안전하게 관리할 것이라는 신뢰를 바탕으로 이동통신 서비스를 이용해 왔습니다. 그러나 피고의 중대한 과실로 인해 이러한 신뢰는 근본적으로 파괴되었으며, 원고들은 더 이상 자신의 개인정보가 안전하게 보호받고 있다는 확신을 가질 수 없게 되었습니다. 이러한 신뢰 상실은 사

회 구성원으로서 느끼는 안정감을 저해하고, 정보화 사회에서의 정상적인 활동에 대한 불안감을 야기하여 원고들의 정신적 안녕을 심각하게 침해하였습니다.

결국, 이 사건 사고는 단순한 정보 유출을 넘어, 정보화 사회에서 개인의 자율성과 존엄성을 보장하는 핵심적인 기본권인 개인정보 자기결정권과 사생활의 비밀과 자유를 정면으로 침해한 중대한 사건입니다. 이러한 기본권 침해로 인한 정신적 고통은 이루 헤아릴 수 없을 정도로 크다 할 것이며, 이는 마땅히 금전적으로 위자되어야 합니다.

5. 손해배상의 범위

가. 일반 손해배상(위자료) 청구

원고들이 이 사건 사고로 인하여 입은 극심한 정신적 고통은 금전적으로 정확히 산정하기는 어려우나, 다음과 같은 이 사건 사고의 제반 사정을 종합적으로 고려할 때, 피고는 원고들에게 그에 상응하는 위자료를 지급할 의무가 있습니다.

1) 청구 금액 : 각 500,000원

원고들은 이 사건 사고로 인한 정신적 손해에 대한 배상으로 피고에 대하여 각자 금 500,000원의 위자료 지급을 청구합니다.

2) 산정 근거

위 위자료 액수는 다음의 사정들을 종합적으로 참작하여 산정한 최소한의 금액

입니다.

가) 피고의 지위 및 그에 따른 고도의 책임

피고는 국내 최대 이동통신사업자로서 국가 기간통신망의 중요한 부분을 담당하며, 수천만 명에 달하는 국민들의 민감한 개인정보 및 통신 관련 중요 정보를 처리·보관하고 있는바, 그 정보의 안전한 관리에 대하여 일반적인 개인정보처리자보다 훨씬 더 높은 수준의 사회적 책임과 고도의 주의의무를 부담합니다. 그럼에도 불구하고 피고는 이러한 책임을 방기하여 대규모 정보 유출 사고를 야기하였습니다.

나) 유출된 정보의 극도의 민감성과 2차 피해의 심각한 위험성

이 사건 사고로 유출된 정보에는 단순 식별 정보를 넘어, 가입자식별번호(IMSI), 유심카드 일련번호(ICCID), 단말기 고유식별번호(IMEI) 등 유심 복제에 직접 악용될 수 있는 핵심 정보가 포함되었으며, 심지어 통신 암호화의 핵심인 '유심 비밀키(K)'와 같은 절대적 인증 정보까지 유출되었을 가능성이 매우 높습니다. 이는 명의도용, 금융사기, 사생활 침해 등 회복 불가능한 2차 피해를 야기할 수 있는 극도로 심각한 위험성을 내포하고 있습니다.

다) 피고의 명백하고 다층적인 법규 위반 행위 및 그로 인한 중과실

피고는 개인정보보호법 및 정보통신망법상 부과된 개인정보 안전성 확보조치 의무를 현저히 해태(약 3년간 악성코드 감염 방치, 최소 23대 서버 감염, 25종 악

성코드 발견, IMEI 유출 은폐 시도 등)하였을 뿐만 아니라, 사고 발생 후 정보주체 및 관계 기관에 대한 통지·신고 의무를 지연하고, 피해 최소화를 위한 적극적인 조치를 소홀히 하는 등 다층적이고 명백한 법규 위반 행위를 저질렀습니다. 이는 단순 과실을 넘어선 중과실에 해당할 가능성이 매우 높습니다.

라) 라) 원고들이 겪는 정신적 고통의 깊이와 지속성

원고들은 자신의 개인정보가 무방비 상태로 노출되었다는 사실, 언제든 심각한 2차 피해의 대상이 될 수 있다는 현실적인 공포감, 평온한 일상생활의 심각한 방해, 피고의 무책임한 사후 대응으로 인한 분노와 무력감 등으로 인해 극심하고 지속적인 정신적 고통을 겪고 있으며, 이러한 고통은 단기간에 해소되기 어려울 것으로 예상됩니다.

마) 피고가 이 사건 유출 사고 후 피해 회복 및 구제를 위해 기울인 노력의 현저한 미흡

피고는 사고 발생 이후에도 피해 사실을 축소·은폐하려는 듯한 태도를 보이거나, 피해자들의 불안감을 해소하고 실질적인 피해를 구제하기 위한 적극적이고 진정성 있는 노력을 충분히 기울이지 않았습니다. 이는 피해자들의 고통을 외면하고 책임을 회피하려는 모습으로 비춰져 원고들의 정신적 고통을 더욱 가중시켰습니다.

바) 유사 사건과의 비교 및 정보 유출의 심각성 증대

과거 다른 개인정보 유출 사건들과 비교하더라도, 이 사건은 유출된 정보의 종

류(IMEI, 유심 비밀키(K) 유출 가능성 등)와 그로 인한 잠재적 피해의 심각성 면에서 전례를 찾기 어려울 정도로 중대합니다. 디지털 사회에서 개인정보의 가치와 중요성이 날로 증대되고 있는 상황을 고려할 때, 이와 같은 대규모 핵심 인증 정보 유출 사고에 대해서는 그에 상응하는 엄중한 책임이 부과되어야 합니다.

사) 소결

위와 같은 제반 사정을 종합적으로 고려할 때, 원고들이 청구하는 각 금 500,000원의 위자료는 이 사건 사고로 인한 원고들의 정신적 고통을 일부나마 위자하기 위한 최소한의 금액이라 할 것입니다.

나. 법정손해배상 청구로의 변경 가능성

만약 본 소송의 진행 과정에서 원고들이 이 사건 사고로 인하여 입은 구체적인 손해액을 입증하는 것이 사실상 극히 곤란하다고 재판부가 판단할 경우, 원고들은 개인정보보호법 제39조의2에 따른 법정손해배상 청구로 변경할 의사가 있음을 미리 밝힙니다.

개인정보보호법 제39조의2 제1항은 “정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.” 라고 규정하고 있습니다.

이 사건 사고는 피고의 중대한 과실로 인하여 원고들의 민감한 개인정보 및 핵심 인증 정보가 대량으로 유출된 사안으로서, 그로 인한 원고들의 정신적 고통은 명백하나 개개인의 구체적인 손해액을 일일이 산정하고 입증하는 데에는 현실적인 어려움이 따를 수 있습니다.

따라서 재판부가 원고들이 입은 손해의 구체적인 액수 입증이 곤란하다고 인정하는 경우, 원고들은 위 법정손해배상 규정에 따라 법원이 이 사건 사고의 경위, 유출된 정보의 종류와 민감성, 피고의 과실 정도, 원고들이 입은 정신적 고통의 정도 등 제반 사정을 참작하여 300만원 이하의 범위 내에서 상당하다고 인정하는 금액의 배상을 구할 것입니다. 이 경우에도 피고는 자신의 고의 또는 과실이 없음을 스스로 입증하지 아니하면 그 책임을 면할 수 없습니다.

원고들은 이처럼 법정손해배상 제도를 통해 신속하고 실효적인 피해 구제가 이루어지기를 희망하며, 이는 개인정보 침해로 인한 피해자의 권리 구제를 용이하게 하고 개인정보처리자의 책임을 강화하고자 하는 개인정보보호법의 입법 취지에도 부합하는 것입니다.

다. 징벌적 손해배상 청구의 고려

원고들은 향후 본 소송의 진행 과정에서 피고의 이 사건 사고 발생 및 사후 대응에 있어서의 고의 또는 중대한 과실의 정도가 더욱 명확하게 입증될 경우, 개인정보보호법 제39조 제3항에 따른 징벌적 손해배상 청구를 추가하거나 기존 청구를 변경하는 것을 적극적으로 검토할 것입니다.

개인정보보호법 제39조 제3항은 “개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 5배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다.” 라고 규정하고 있으며, 같은 조 제4항에서는 법원이 징벌적 손해배상액을 정할 때 ① 고의 또는 손해 발생의 우려를 인식한 정도, ② 위반행위로 인하여 입은 피해 규모, ③ 위반행위로 인하여 개인정보처리자가 취득한 경제적 이익, ④ 위반행위의 기간·횟수, ⑤ 개인정보처리자의 재산상태, ⑥ 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도, ⑦ 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도 등을 고려하도록 하고 있습니다.

이 사건에서 피고는 다음과 같은 사정으로 볼 때, 단순 과실을 넘어선 고의에 준하는 악의적인 의무 해태 또는 중대한 과실이 인정될 여지가 충분하다고 판단됩니다.

첫째, 장기간에 걸친 심각한 보안 시스템 방치 및 관리 소홀입니다. 과기정통부 2차 조사결과에서 드러난 바와 같이, 피고의 일부 서버는 약 3년간 악성코드에 감염된 채 방치되었고, 최소 23대의 서버가 감염되었으며 25종의 악성코드가 발견되었습니다. 이는 피고가 정보보호에 대한 기본적인 투자와 관리를 극도로 소홀히 하였음을 명백히 보여주며, 이러한 장기간의 방치는 미필적 고의에 가깝거나 적어도 중대한 과실에 해당한다고 볼 수 있습니다.

둘째, IMEI 유출 사실 은폐 및 축소 시도 등 기만적인 사후 대응입니다. 피고는

사고 초기 IMEI 유출 가능성을 부인하다가 정부 조사 결과가 나온 이후에야 마지못해 인정하는 등 피해 사실을 축소·은폐하려는 듯한 태도를 보였습니다. 이는 정보주체와 규제 당국을 기만하려는 의도가 있었다고 볼 수 있으며, 이러한 행위는 징벌적 손해배상액 산정 시 불리한 요소로 고려될 수 있습니다.

셋째, 국내 최대 이동통신사업자로서의 사회적 책임과 의무의 극명한 방기입니다. 피고는 막대한 이익을 창출하는 대기업이자 국가 기간통신망 사업자로서 일반 기업보다 훨씬 더 높은 수준의 정보보호 의무와 사회적 책임을 부담합니다. 그럼에도 불구하고 전례 없이 심각한 개인정보 유출 사고를 야기하고 그에 대한 책임 있는 자세를 보이지 않는 것은 그 비난 가능성이 매우 크다고 할 것입니다.

넷째, 피해자 구제를 위한 노력의 현저한 미흡입니다. 피고는 이 사건 사고 이후에도 피해자들의 불안감을 해소하고 실질적인 피해를 구제하기 위한 적극적이고 진정성 있는 노력을 충분히 기울이지 않았습니다. 이는 개인정보보호법 제39조 제4항 제7호에서 정한 '정보주체의 피해구제를 위하여 노력한 정도'가 매우 미흡함을 의미하며, 징벌적 손해배상의 필요성을 뒷받침합니다.

만약 추후 증거 조사를 통해 위와 같은 피고의 고의 또는 중대한 과실이 더욱 명백히 드러나고, 피고가 이 사건 사고를 통해 부당한 비용 절감 등의 경제적 이익을 얻은 정황 등이 확인된다면, 이는 악의적인 개인정보 침해 행위에 대한 제재 및 유사 사고 재발 방지라는 징벌적 손해배상 제도의 취지에 비추어 볼 때 마땅히 그 책임이 가중되어야 할 것입니다. 따라서 원고들은 재판 진행 상황에 따라 징벌적 손해배상 청구를 통해 피고에게 더욱 강력한 책임을 물을 것임을 밝힙니

다.

6. 결론

이상에서 상세히 살펴본 바와 같이, 피고는 국내 최대 이동통신사업자로서 원고들을 포함한 수많은 가입 고객들의 개인정보를 안전하게 관리하여야 할 고도의 법적·사회적 책무가 있음에도 불구하고, 개인정보보호법 및 정보통신망법상 부과된 개인정보 보호조치 의무, 침해사고 발생 시 정보주체 및 관계 기관에 대한 통지·신고 의무, 유출에 따른 피해 최소화 조치 의무 등 각종 중대한 의무들을 명백히 위반하였습니다.

특히, 피고는 약 3년간 악성코드 감염 사실을 인지하지 못한 채 핵심 서버들을 방치하였고, 그 결과 원고들의 휴대전화번호, 가입자식별번호(IMSI), 유심카드 일련번호(ICCID)는 물론, 스마트폰의 고유 식별 정보인 단말기 고유식별번호(IMEI)까지 대량으로 유출되었으며, 통신 암호화의 핵심인 '유심 비밀키(K)'와 같은 절대적 인증 정보의 유출 가능성까지 제기되는 등 전례 없이 심각한 개인정보 유출 사고를 야기하였습니다.

더욱이 피고는 이 사건 사고 발생 이후에도 유출 사실 및 그 범위를 축소·은폐하려 하거나, 피해자들에 대한 통지 및 관계 기관 신고를 지연하고, 피해자들의 불안감을 해소하고 실질적인 피해를 구제하기 위한 적극적이고 진정성 있는 노력을 다하지 않는 등 무책임한 태도로 일관하여 원고들의 정신적 고통을 더욱 가중시켰습니다.

개인정보보호법 제39조 제1항 제2문에 따라 피고는 이 사건 사고 발생 및 그로 인한 원고들의 손해 발생에 있어 자신에게 고의 또는 과실이 없음을 스스로 입증하지 못하는 한 그 책임을 면할 수 없습니다. 그러나 앞서 적시한 제반 사정들에 비추어 볼 때 피고의 중대한 과실은 명백하며, 피고가 무과실을 입증하는 것은 사실상 불가능하다고 할 것입니다.

이로 인하여 원고들은 자신의 개인정보가 심각하게 침해당하였을 뿐만 아니라, 유심 복제, 명의 도용, 금융 사기 등 2차 피해 발생에 대한 극심한 불안감과 공포심, 평온한 일상생활의 심각한 방해, 피고에 대한 신뢰 상실 등 이루 말할 수 없는 정신적 고통을 겪었으므로, 피고는 원고들에게 그로 인한 손해를 배상할 책임이 있습니다. 이러한 피고의 책임과 피해자들에 대한 충분한 배상의 필요성은 대한변호사협회 역시 2025. 4. 30.자 성명서를 통해 이 사건 개인정보 유출 사태의 심각성을 지적하며 강력히 촉구한 바이기도 합니다.[5)]

또한, 피고는 개인정보보호법 제39조의7에 따라 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 할 의무를 부담하는 사업자인바, 이러한 책임 이행 능력을 바탕으로 원고들의 피해를 신속하고 성실하게 전보하여야 할 것입니다.

따라서 피고는 원고들에게 이 사건 사고로 인한 정신적 손해에 대한 위자료로서 각자 금 500,000원 및 이에 대하여 이 사건 유출사고 발생일인 2025. 4. 18.부터 이 사건 소장 부본 송달일까지는 민법 소정의 연 5%의, 그 다음 날부터 다 갚

5) 갑 제6호증, 대한변호사협회 성명서

는 날까지는 소송촉진 등에 관한 특례법 소정의 연 12%의 각 비율에 의한 지연손해금을 지급할 의무가 있다 할 것입니다.

원고들은 재판부의 현명한 판단을 통해 이 사건 사고로 인한 피해가 조금이나마 회복되고, 향후 이와 같은 불행한 사태가 재발하지 않도록 경종을 울리는 계기가 마련되기를 간절히 바랍니다.