암호화폐, 가상화폐 투자사기 분쟁 사례 – 신규 암호화폐 투자, 가치하락, 투자금회수불가 상황 - 사기로 인한 손해배상책임 인정 but 투자자의 40% 책임 분담: 서울중앙지방법원 2017. 9. 29. 선고 2016가단5071771 판결

판결요지: "피고는 가상화폐인 유토큰에 투자를 직접적으로 권유하고 그 과정에서 객관적 근거도 없이 유토큰이 매일 1% 이상씩 가치가 상승한다는 이례적인 전망을 수익예상의 근거로서 제시하면서 투자를 권유한데가

법정화폐와 달리 환전이 되지 않는 가상화폐의 특성상 투자 회수를 위해서는 판매자를 통해 직접 환전을 할 수밖에 없음에도 피고는 본인이 직접 환전을 해주겠다고 해 사실상 투자금 일부의 조기 회수도 약속해줌으로써 이와 같은 환상적인 수익전망과 함께 그 회

수의 현실적 가능성을 함께 믿은 투자자 원고가 유토큰 매입을 위한 거래를 한 것이고,

이후 피고가 제시한 전망과 달리 유토큰은 시세가 현저히 하락해 거래도 되지 않는 상태로 전락한데다가 환전도 이루어지지 않아서 투자자 원고는 투자금을 회수할 수 없는 상태에 빠져서 같은 금액 상당의 손해를 입게 된 것이다.

피고는 당시 유토큰 투자의 근거가 되는 향후 전망에 관해 현실적으로 실현이 어렵다는 점을 미필적으로나마 인식하고 있었던 것으로 보이므로 그에 관한 투자유치 및 투자금 수수 등의 일련의 행위와 관련하여 이루어진 불법행위로 인한 투자자 원고가 입은 손해를 배상할 의무가 있다.

다만 법원은 "투자자 원고도 상품·운영자 등에 대해 충분히 검토하지 않은 채 수익의 실현 가능성만을 기대하고 성급히 투자한 과실이 있다"면서 투자자의 책임을 40% 인정하고, 피고의 책임을 60%로 분배하였습니다.

암호화폐, 가상화폐 거래소를 상대로 하는 해킹사고 관련 민사소송 여부 - KT의 개인정

보 해킹사고에 대한 손해배상책임 불인정 판결 등 고려

가상화폐 거래소를 대상으로 하는 소송의 원인으로는 투자자 개인정보에 관련 해킹, 가상화폐 자체에 관한 해킹, 거래접속폭주로 인한 서버다운 등으로 매도매입 거래불능 또는 접속불능 사안이 중요합니다. 기타 서버장애와 관련된 여러가지 사안도 소송대상으로 거론되는 것 같습니다.

해킹사고 발생원인이 거래소의 시스템 자체 또는 직원의 관리부실로 인한 경우라면 거래소는 그 책임을 면하기 어렵습니다. 직원이 개인정보보호법 등 관련 법령 및 회사의 관리규정을 위반한 경우, 해당 직원의 개인적 책임은 물론 사용자인 거래소 회사가 정보통신망법 및 개인 정보 보호법에서 정한 적절한 개인 정보 보호 정책을 수립 및 실시하지 않았거나, 직원에 대한 개인 정보 교육을 실시하지 않은 경우에 해당하여 거래소에 대해 법령상 관리책임위반으로 인한 손해배상책임을 물을 수 있습니다.

거래소에서 투자자의 주민등록번호, 비밀번호를 암호화하는 등 일정한 보안조치를 취한 것은 맞지만, 직원이 작업을 위해 일시적으로 개인업무용 PC에 저장하고 있다가 해킹을 당한 경우, Log out을 하지 않고 퇴근하였거나 직원 PC에 보안백신 등이 설치되어 있지

않았다면, 사용자인 거래소 또한 관련 법령 위반으로 인한 책임을 면하기 어려울 것입니다.

한편, 거래소와 직원들이 관리책임을 다했지만, 거래소에서 적용한 기술적 보호조치가 충분했는지도 중요한 쟁점입니다. 거래소가 관련 법령에서 요구하는 기술적 보호조치를 다하지 않았다면 관리책임과 무관하게 기술적 조치위반으로 인한 손해배상책임을 물을 수 있습니다.

이때 기술적 보호조치의 수준과 내용이 중요합니다. 거래소가 해킹사고를 막지 못했다고 해서 모든 경우에 무조건 책임을 묻는 것은 아닙니다. 해킹사고와 관련된 기술적 조치와 책임문제와 관련하여 최근에 나온 KT 항소심 판결이 좋은 사례로 생각되므로 간략하게 소개합니다.

종래 발생한 개인정보 유출사고 중 외부로부터의 해킹이 관여된 사건의 판결을 보면, 서비스 운영자, 개인정보처리자에게 법적 책임을 추궁하는 것이 쉽지 않다는 것을 알 수 있습니다. 예를 들어, 2012년 KT 가입자 870만명의 개인정보가 해킹으로 유출된 사고가 있었는데, KT에서는 5개월 동안 해킹사실을 모르고 있다가 내부 보안점검을 통해 해킹

사실을 파악했다고 합니다. 이에 개인정보 유출피해자들이 KT의 관리부실로 개인정보가 유출됐다고 손해배상책임을 묻는 소송을 제기하였습니다.

1심 법원은 기술적 보호조치가 미흡했다고 KT의 책임을 일부 인정하였으나, 최근 항소심 판결(2015나61155)에서는 1심 판결을 뒤집고 KT의 책임을 전면 부인하였습니다. 항소심 판결요지를 간략하게 인용하면 다음과 같습니다. "KT가 개인정보 유출방지에 관한 기술적·관리적 보호조치를 이행하지 않은 과실로 인해 사고가 발생했다고 보기 어렵다. KT는 규정을 준수해 접속기록을 확인해왔다고, 해커가 정상적 서버를 우회해 접속기록을 남기지 않고 정보를 유출했을 가능성을 예상하기 어려웠다. 인터넷이라는 특성상 모든 사이트가 해커의 불법적인 침입에 노출될 수밖에 없고 완벽한 보안을 갖추기는 어렵다."

직원의 확실한 관리부실 사실이 없음에 불구하고 발생한 해킹사고에 대해서는 가상화폐 거래소에 대해 기술적 보호조치 미흡 등을 이유로 하는 손해배상책임을 추궁하는 것이 만만하지 않을 것임을 시사합니다.

또한, 마찬가지로 일시적 접속폭주로 인한 서버다운과 관련된 가상화폐 거래소의 책임 또한 쉽게 인정받을 가능성은 매우 낮습니다. 기술적 보호조치 사례와 유사한 쟁점입니

다.

거래소의 이용약관에 '가상화폐 발행 관리 시스템 또는 통신 서비스업체의 서비스 불량으로 인해 가상화폐 전달에 하자가 발생한 경우는 책임을 지지 않는다'고 손해배상 면책 조항을 두고 있다고 합니다. 계약법상 책임을 묻는다면 만나게 될 또 하나의 난관입니다.

한편, 가상화폐 거래소 상대 소송의 진정한 난제는, 우리나라 법원이 가상화폐의 법적성질을 어떻게 파악하고 그 가치를 인정할 것인지, 서버접속불능 사고 즈음에 발생한 가상화폐의 시가 급락으로 인한 손실을 인정할지, 매매성립 가능성과 손실의 인과관계를 인정할지 등 가상화폐의 법적성질에 관한 사안입니다.