Medidata Solutions, Inc. v. Federal Ins. Co.

Year: 2018
Court: U.S. Court of Appeals, 2nd Circuit
Case Number: 17-2492-cv

Businesses are increasingly looking to their property and liability insurance policies for indemnification and defense in connection with cyber crimes including data breaches, hacks and ransomware demands. Insurance companies are taking varying approaches to accepting and rejecting these claims. UP is weighing in to support coverage for business losses due to cyber crime, and working with state insurance regulators. Our goal: A transparent marketplace where businesses can buy fairly priced policies that will meet their reasonable expectations of coverage for losses due to cyber incidents. An insurance policy's coverage grant must be interpreted in a broad sense, as to afford coverage to the insured where reasonable. If an insurer wishes to exclude coverage for certain types of losses, it must do so in clear, unmistakable language. Under a proximate cause analysis in New York, where a series of related, connected actions combine to cause loss, there must be coverage, even where the policy requires "direct physical loss." UP reminded the Court that insurance policies are contracts of adhesion, offered to the policyholder on a take-it-or-leave basis. Here, specifically, the insurer argued that it's computer crime/fraud coverage required brute-force hacking and would not pay for losses resulting from an employee's unauthorized transfer of funds to a third party, induced by fraudulent impersonation. UP argued that under the District Court's [correct] causation analysis, such losses are direct losses resulting from "manipulation of a computer system" which would comport with the policyholder's reasonable expectations of coverage.

UP's brief was authored pro bono by Joshua Gold, Esq., Dennis J. Nolan, Esq., and Peter A. Halprin, Esq. of Anderson Kill, P.C.