Victory for Pharma Giant Merck in NotPetya Cyber Attack Suit Redefines “Act of War” Insurance Claims

CPO Magazine

A long-simmering suit involving pharmaceutical giant Merck and the 2017 NotPetya cyber attack has finally been ruled on, and the victory for Merck means that cyber insurers now have much less ground to stand on when denying insurance claims on an “act of war” basis.

Merck sued several of its insurers that denied its insurance claims on the basis of the NotPetya cyber attack being viewed by them as an act of war, coming as it did in the midst of conflict between Russia and Ukraine. A New Jersey court has ruled that the situation did not rise to the standards of that exception, and that some collective $1.4 billion in Merck losses from the incident will have to be covered.

Court finds for Merck, ransomware damage insurance claims must be paid

NotPetya was meant to strike Ukrainian businesses, but spread beyond its intended targets to cause some $10 billion in damages around the world. Merck saw some 40,000 of its computers damaged by the ransomware during the incident, and an early 2022 ruling established that the company suffered over $1 billion in damage between its equipment replacement, business outages and outside contractors brought in for remediation. The more recent ruling affirms that the “War or Hostile Acts” exclusion listed in company policies does not apply to the NotPetya cyber attack.

One of the court’s central findings was that if there is any ambiguity in the language of an insurance policy, the interpretation should meet the “reasonable expectations” of the policy holder. Act of war policies have the established purpose of protecting the insurer from the widespread devastation that can

occur when one country undertakes military action against another; for example, most automobile owners are out of luck if a foreign power happens to bomb their car during a conflict.

But one of the general standards is that at least one side in the conflict must declare war on the other, something that obviously did not happen here as even Russia and Ukraine were operating under some of the terms of the Minsk agreements at the time. The Russian government also continues to deny responsibility for the NotPetya cyber attack, even though much of the rest of the world has confidently attributed it to them. These terms were also drafted long before computers were in homes, and long before "cyber warfare" was even a concept that insured parties would even consider.

The ruling does not change any laws, and will only directly pertain as a precedent to insurance claims under dispute in New Jersey courts. However, rulings on similar cases in other jurisdictions could turn to this one as a basis of legal thinking, as it is the first of its kind involving insurance claims and this sort of war exception.

NotPetya cyber attack ruling could serve as model for "spillover" damage caused by nation-state hackers

Regardless of the limited scope of legal application at present, the NotPetya cyber attack ruling will also likely prompt cyber insurers to revise the language in their policies to cover their bases. Judge Thomas J. Walsh's opinion on the ruling specifically noted the failure of the insurers to change the policy language to include "non-traditional" forms of warfare.

However, the NotPetya cyber attack ruling is not just about inadequate contract wording. Walsh also referred to a 1922 decision involving a collision between two ships during World War I that found "remote consequences" of a war cannot automatically be considered an act of war even if the war was a proximate cause in some way.

David Cummings, who co-authored an amicus brief filed by United Policy holders in the case, expands on the judge's perspective: "The Appellate Division's decision is an important win for policyholders who continue to seek (and pay substantial premiums for) certainty with respect to their insurance coverage in the face of these oft-uncertain cyberattacks. In many ways, this decision boils down to the Court's thoughtful application of fundamental principles of insurance law: exclusionary provisions must be

construed narrowly against the insurer, any ambiguities must be resolved in the insured's favor and consistent with the insured's reasonable expectations. On that score, the Court correctly determined that the plain language of the policies' hostile/warlike action exclusion simply cannot reasonably be interpreted as encompassing a cyberattack on a non-military company providing commercial services to non-military customers. The mere presence of hostile or warlike action is not enough where, as here, the underlying activity is commercial in nature, and the damage is not caused by a warlike attack directed at the policyholder. In sum, the Court's decision was a meaningful affirmation that plain language and the core, policyholder-friendly tenets of insurance law must ultimately prevail."

The NotPetya cyber attack case is just one in a recent collection that has tended to favor those filing insurance claims over the insurers, as previously gray areas of the cyber world begin to be colored in with precedent. Among other things, recent decisions have established that ransomware attacks do not have to be catastrophic to the point of business stoppage to meet the threshold for filing an insurance claim. This is not necessarily a net positive for insurance buyers, however, as the response from insurers is an increasingly sharp tightening and reduction of coverage. Cyber insurance has become increasingly difficult to get over roughly the past two years, and when it is obtained the coverage is usually not as good and the contract language not as favorable. Some insurers have simply decided to go with the "nuclear option" and drop ransomware coverage entirely.

Monica Oravcova, COO and co-founder of Naoris Protocol, believes the action prompted by this decision will be immediate and severe, though the cyber insurance market has already contracted considerably in a very short amount of time: "This is an incredible blow for the insurance industry and no doubt will precipitate a flurry of activity in existing insurance industry underwriting practices. Lloyds of London have already paved the way in terms of dealing with the fallout of ambiguous policy language by requiring insurers to craft exclusionary clauses for "acts of war" which was the hotly debated theme of the lawsuit. The effect of the ruling will impact not only insurers but the companies that seek cover. We can expect even tighter restrictions, exclusions and possibly another spike in premiums. Now more than ever, we need to look to decentralised technology to prevent these attacks as the costs both in terms of productivity and economics, are becoming a trillion dollar headache for business and government".