LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

FRIDAY, JUNE 16, 2023

PERSPECTIVE

Antiquated war exclusion does not bar coverage for $700M cyber insurance claim

By Robert Wallan and John Chamberlain

Does a devastating computer virus attack, that might be sponsored by a nation state, qualify as "hostile or warlike" action within the meaning of a war risk exclusion that was drafted centuries before the advent of modern computers? Clearly not, said a three judge-panel of New Jersey's Appellate Division, over the objections of a bevy of insurance carriers who argued that the word "hostile" in the hoary exclusion was broad enough to encompass cyber-attacks. The decision – *Merck & Co. v. Ace Am. Ins. Co.*, No. A-1879-21, 2023 WL 3160845 (May 1, 2023) – is a triumph for common sense, plain English, and for policyholders nationwide, and a crucial check on an insurance industry that has taken increasingly aggressive positions in the fast-developing area of cyber insurance law.

The plaintiff, Merck, is a multinational pharmaceutical company that fell victim in June 2017 to the now-infamous "NotPetya" computer virus, which utilized a backdoor in otherwise-legitimate accounting software to circumvent traditional anti-virus protections. According to the court, "[w]ithin ninety seconds of the initial infection, approximately 10,000 machines in Merck's global network were infected by NotPetya," and "[u]ltimately, over 40,000 machines in Merck's network were infected," causing massive disruptions to Merck's business. Merck sought coverage under its all-risk property insurance program (which specifically extended to computer virus attacks), seeking reimbursement of a staggering $699,475,000 in losses from the event. The insurance carriers retained an expert consultant, who concluded "with high confidence" that the virus attack "was very likely orchestrated by actors working for or on behalf of the Russian Federation." Clinging to this speculative conclusion, Merck's carriers denied coverage under the policies' war risk exclusions for losses "caused by hostile or warlike action … by any government or sovereign power … or by an agent of such government [or] power."

Merck disputed the carriers' attribution theory, but both the trial court and the Appellate Division deemed the dispute immaterial because the virus attack did not fall within a fair reading of the exclusionary clause, regardless of who sponsored it. As the trial court found: "[N]o court has applied a war (or hostile acts) exclusion to anything remotely close to the facts herein. The evidence suggests that the language used in these policies has been virtually the same for many years." And despite the modern prevalence of cyber attacks, the "Insurers did nothing to change the language of the [exclusion] to reasonably put this Insured on notice that it intended to exclude cyber attacks," meaning "Merck had every right to anticipate that the exclusion applied only to traditional forms of warfare."

The Appellate Division affirmed, emphasizing the plain language of the policy and traditional rules of policy construction. Invoking the familiar rule that "[i]nsurance policy exclusions must be construed narrowly," the Court rejected the insurers' argument that "the word 'hostile' should be read in the broadest possible sense, as meaning 'adverse,' 'showing ill will or a desire to harm,' 'antagonistic,' or 'unfriendly.'" Importantly, where a policy affirmatively covers war risks, the converse rule applies: courts interpret coverage grants expansively and exclusions narrowly, resolving any ambiguities in favor of coverage.

Coverage "could only be excluded here if [the court] stretched the meaning of 'hostile' to its outer limit in an attempt to apply it to a cyber-attack on a noncombatant firm that provided accounting software updates to various noncombatant customers, all wholly outside the context of any armed conflict or military objective." In the court's view, that approach would conflict with "basic construction principles requiring a court to narrowly construe an insurance policy exclusion." The plain meaning of an exclusionary word or phrase did "not equate to its broadest possible interpretation" – as the carriers contended – "but rather its narrowest." Thus, "the plain language of the exclusion did not include a cyberattack on a non-military company that provided accounting software for commercial purposes to non-military consumers, regardless of whether the attack was instigated by a private actor or a 'government or sovereign power.'"

Robert Wallan *is a partner, and* **John Chamberlain** *is counsel at Pillsbury Winthrop Shaw Pittman LLP.*

The exclusion "require[d] the involvement of military action" to be triggered – a key limitation.

The decision is a resounding victory for Merck and a critical precedent for policyholders nationwide. A similar case settled last fall without judicial guidance on the application of the war risk exclusion. *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018L011008 (Ill. Cir. Ct. 2018). The Merck decision is both well-reasoned and anchored in common law principles shared by all U.S. jurisdictions, making it an imposing and highly persuasive precedent even in jurisdictions where it is not binding.

Unfortunately, the insurance industry continues to pursue the sale of policies that rarely provide coverage. In response to their failure to have courts rewrite their policies, insurance carriers have already begun adding language broadening the scope of the war risks exclusion and excluding state sponsored-cyber attacks. For example, Chubb (or ACE, one of the losing parties in the Merck decision) has amended its war risk exclusion to specifically exclude "Malicious Computer Act(s)," in addition to "any hostile event or act." In other words, if you think you are buying coverage to protect against cyber attacks and malware, it will be critical to read the actual policy language in advance for new exclusions that may swallow most coverage you might think you are buying.

Similarly, the London market has drafted new exclusionary language for "cyber operations" attributable to state actors. Somewhat curiously, the London exclusions recite that the "primary but not exclusive factor" in determining attribution is "whether the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located attributes the cyber operation to another state or those acting on its behalf." This is extraordinary in that it assumes the accuracy of a host state's determination, even though misdirection and obfuscation are hallmarks of spycraft, and despite that not all nation states should be expected to be honest brokers in this area. A savvy government could attempt to avoid the exclusion's application to businesses within its borders by publicly attributing an attack to something other than state actors, even if the government's "intelligence and security services" have actually determined otherwise.

Policyholders going to market or up for renewal should carefully scrutinize the scope of coverage and the excluded war risks to ensure they understand the coverage being offered. Assuming that cyber insurance coverage provides protection from cyber attacks could prove to be a mistake.