Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Mondelez's $100M Fight With Zurich May Curb Hack Coverage

By **Jeff Sistrunk**

Law360 (January 18, 2019, 2:49 PM EST) -- Mondelez International Inc. is battling Zurich American Insurance Co. over coverage for $100 million in losses the snack food giant suffered in a 2017 cyberattack that the U.S. and its allies blamed on Russia, and experts say a ruling permitting the insurer to invoke a war exclusion to deny the claim could leave companies uninsured for similar hacks.

In a complaint filed in a Cook County, Illinois, court last October, Mondelez accused Zurich of improperly refusing to pay out under an "all-risks" property insurance policy for financial losses it suffered in the sweeping "NotPetya" cyberattack, which the CIA and sister agencies in the United Kingdom, Australia and Canada have attributed to hackers affiliated with the Russian military.

The suit said Zurich based its coverage denial on a policy exclusion for losses or damage resulting directly or indirectly from "a hostile or warlike action in time of peace or war" carried out by a government, sovereign power or military force. Mondelez called Zurich's argument "unprecedented," and asserted that, in the past, similar war risk exclusions had never been applied to "anything other than conventional armed conflict or hostilities."

Given the uptick in hacking incidents attributed to hostile government agents, a decision adopting Zurich's interpretation of the war exclusion could give more insurers ammunition to deny policyholders' claims for cyberattack coverage under both traditional and specialized cyber insurance policies containing identical or similar exclusions, according to some attorneys interviewed by Law360.

"These are legacy exclusions from older policies that had not envisioned this electronic day and age," said Farella Braun & Martel LLP partner Tyler Gerking, who represents policyholders. "Most — if not all — insureds would be surprised by an insurer's application of this exclusion because it would seem to eliminate coverage that the insured intended to buy."

Conversely, Joshua Mooney, co-chair of White and Williams LLP's cyber law and data protection group, said Mondelez's assertion that Zurich's coverage denial is unprecedented "lacks merit." The fact that the war exclusion in Zurich's policy contains older language predating the age of cyber warfare shouldn't cut against the insurer's position, he said.

"Courts are frequently called upon to apply legacy language to novel sets of facts when rendering coverage decisions," said Mooney, who represents insurers. "Anyone who has litigated coverage for privacy, pollution or computer fraud claims will know that."

The roots of the coverage dispute date to June 2017, when two of Mondelez's servers were infected with NotPetya malware, according to the company's complaint. The malicious code spread across Mondelez's network and ultimately "rendered permanently dysfunctional" 1,700 of its servers and 24,000 of its laptops, the suit said.

"As a result of the damage caused both to its hardware and operational software systems, MDLZ incurred property damage, commercial supply and distribution disruptions, unfulfilled customer orders, reduced margins and other covered losses aggregating well in excess of $100 million," Mondelez's attorneys wrote in the complaint, referring to the company by its Nasdaq trading name.

In early 2018, the U.S. and several allies blamed the NotPetya attack, which initially targeted Ukraine's financial, energy and government institutions but spread to businesses across the world because of its "indiscriminate design," on hackers within the Russian military, according to White House statements issued at the time.

For its part, the Kremlin called the accusations "unsubstantiated and groundless," with Kremlin spokesman Dmitry Peskov saying in a February 2018 statement that the charges were part of a "Russophobic campaign that is not based on any evidence."

According to Mondelez's complaint, the company's all-risks policy with Zurich included coverage for "physical loss or damage to electronic data, programs, or software" caused by the "malicious introduction of a machine code or instruction," as well as coverage for extra expenses incurred by Mondelez due to the failure of its "electronic data processing equipment or media to operate."

When Mondelez sought payment of its $100 million claim from Zurich, though, the insurer balked, citing the policy's war exclusion, according to the complaint. After talks between the two broke down, Mondelez sued.

A Zurich spokeswoman said the insurance company does not comment on pending litigation. Mondelez representatives did not immediately respond to a request for comment.

Anderson Kill PC shareholder Joshua Gold, who represents policyholders, told Law360 the dispute is noteworthy "because what had been a theoretical discussion in the industry — would insurance companies invoke the war risk exclusion for a cyber claim — has now been answered.

"This now makes the conversation very real: that cyber risk management must consider what clarity and assurances policyholders can get that insurance companies will not attempt to evade coverage for cyber claims where a state actor is allegedly involved," Gold said.

Gold asserted that history could be on Mondelez's side, because courts dealing with war exclusions in cases involving terrorist incidents targeting the aviation and hospitality industries have tended to construe the exclusionary language narrowly.

"I would expect that kind of approach to be used in this case and perhaps others that follow suit," he said. "If you interpret the exclusion too broadly, you start swallowing up the coverage for damage and loss caused by the 'malicious introduction of a machine code or instruction.'"

According to Gerking of Farella Braun, Zurich may face an uphill battle to marshal definitive evidence tying the infection of Mondelez's servers to Russian agents, which could defeat its reliance on the war exclusion.

"I don't think the insurer is going to get the CIA or [National Security Agency] to testify about their findings, and I also don't think the Russian government is going to be willing to provide evidence," Gerking said. "Therefore, [Zurich is] going to be hard-pressed to come up with concrete proof that a government engaged in this attack, even if there is speculation in the press that the Russian government did it."

On the other hand, White and Williams' Mooney said intelligence officials' public conclusions about Russia's involvement in the cyberattack should be sufficient proof for Zurich to apply the exclusion.

"If anything, MDLZ effectively may have to show that the Russian government wasn't the culprit, which may be an impossible task," he said.

The fact that Mondelez was apparently not an intended target of the attack is irrelevant, Mooney added, because the exclusion broadly bars coverage for any losses directly or indirectly resulting from a hostile or warlike action.

"Thus, MDLZ need not have been a target of the Russian military for the exclusion to apply," he said. "MDLZ suffered collateral damage from the attack, which also falls within the exclusion."

While Mondelez's coverage dispute involves a property policy, war exclusions are also common in specialized cyber insurance policies tailored to hacking and digital risks. If the Illinois court rules in Zurich's favor, insurers may have a difficult time selling cyber policies with such exclusions in the future, unless they also insert exceptions for acts of cyberterrorism, according to attorneys.

"There is a major commercial issue as to whether such exclusions are appropriate in cyber policies," said Clive O'Connell, head of McCarthy Denning Ltd.'s insurance and reinsurance group. "When you talk about cyber risks, there is no safety net for companies to fall back on, so insurance must fill that role. If a given cyber policy contains a war exclusion, that may make a company think twice about accepting that cover."

At the end of the day, O'Connell said, companies want a policy that will respond to cyberattack-related losses regardless of the hacker's identity.

"When it comes to cyber risks, the identity of the attacker doesn't matter to the companies that are targeted," he said. "They don't care if they are attacked by agents of the North Korean government or by a man sitting in his basement in his underwear, tapping away on his laptop."

Mondelez is represented by David M. Kroeger and John H. Mathias of Jenner & Block LLP.

Zurich is represented by Ronald S. Safer and Sondra A. Hemeryck of Riley Safer Holmes & Cancila LLP and Philip C. Silverberg of Mound Cotton Wollan & Greengrass LLP.

The case is Mondelez International Inc. v. Zurich American Insurance Co., case number 2018 L 011008, in the Circuit Court of Cook County, Illinois, County Department, Law Division.

--Editing by Katherine Rautenberg and Orlando Lorenzo.