wiley

ARTICLE

Dealing With 'Relatedness' Under Cyberinsurance Policies

Law360
March 23, 2017

Practice Areas

Privacy, Cyber & Data Governance

When responding to a data breach, companies typically undertake a comprehensive forensic investigation to evaluate the potential extent of the incident, the vulnerabilities that enabled the compromise and the appropriate remediation measures. It is not uncommon for an organization in the process of such an investigation to uncover indicia that a different compromise may have occurred as well. Identifying the existence of a second breach may considerably alter the scope of the organization's response to the first event and may impact any third-party claims in a significant way.

The discovery of a second breach can have meaningful implications for the organization's cyberinsurance coverage. After first analyzing threshold trigger issues under the operative insuring agreements, the starting place for analyzing these issues is under "related claims" policy language, which in effect operates to render two (or more) distinct events or claims to be deemed a single event or claim for purposes of insurance coverage.[1] At the most fundamental level, deeming the claims "related" will dictate whether and to what extent the relevant cyberpolicy will respond. The implications of this analysis include whether: (1) the insured need only satisfy one retention before coverage is triggered; (2) only one limit of liability applies; and (3) events discovered after an operative policy period are deemed to have been discovered previously during an earlier policy period. Relatedness may also bear on other policy provisions that are often implicated by claims under cyberpolicies.

While case law specific to cyberpolicies is still in the early stages of development, there is a large body of authority analyzing relatedness under other types of insurance policies. This authority confirms that

when the relevant policy terms (such as "related" or "interrelated") are defined, courts focus on that language rather than looking to common law definitions as developed through case law. See Nomura Holding Am. Inc. v. Fed. Insurance Co., 629 Fed. App'x 38, 40 (2d Cir. 2015) (affirming district court's conclusion that claims were related but observing that it erred in employing a "factual nexus" test, noting instead that the district court should have simply applied the plain language of the policy). When left undefined, terms such as "related" or "interrelated" are commonly understood and used to broadly encompass both logical and causal connections. See, e.g., Bay Cities Paving & Grading Inc. v. Lawyers' Mut. Insurance Co., 855 P.2d 1263, 1271, 1274 (Cal. 1993). "Relatedness" may not encompass every conceivable logical relationship, however, such as where the link between the claims or events is extremely attenuated. See id. at 1275.

When addressing third-party claims resulting from a series of data breaches, the related claims analysis may be guided by the fact that the claims are premised on a single element of harm or by a single cause. Many courts find these factors significant in assessing relatedness. See, e.g., Kilcher v. Cont'l Cas. Co., 747 F.3d 983 (8th Cir. 2014) (wrongful acts asserted against a financial adviser by different claimants in a series of different claims were logically connected because the insured engaged in the same method or modus operandi, notwithstanding that each claimant met with the insured separately; invested different amounts in different life insurance products; invested at different times over many years; and suffered losses in different amounts); WFS Financial Inc. v. Progressive Cas. Insurance Co. Inc., 232 Fed. App'x 624, 625 (9th Cir. 2007) (suits "filed by two different sets of plaintiffs in two different fora under two different legal theories" involved interrelated wrongful acts because they were both premised on the insured's alleged "business practice" with respect to the mark-up of the insured's loans); Brecek & Young Advisors Inc. v. Lloyds of London Syndicate 2003, 715 F.3d 1231, 1239 (10th Cir. 2013) (applying New York law) (concluding that claims arising from a common scheme were "interrelated"); but see, e.g., Am. Guar. & Liab. Insurance Co. v. Chicago Insurance Co., 105 A.D.3d 655, 656-57 (N.Y. App. Div. 2013) (holding that claims from senior citizens who all responded to the attorney's mass market mail campaign and later lost money when the attorney referred them to a financial services representative who in turn stole their money were not the "same or related" because the attorney "provided separate services to multiple clients"); Nat'l Union Fire Insurance Co. of Pittsburgh, Pa. v. Ambassador Grp. Inc., 691 F. Supp. 618, 623-24 (E.D.N.Y. 1988) (interpreting "interrelated acts" language as not applying to common "mismanagement" of company, instead highlighting that the claims involved "legally distinct claims that allege different wrongs to different people").

Relatedness in the context of first-party cybercoverage involves a similar (albeit distinct) analytical framework. The key difference is that the inquiry does not look to the allegations of the claims — because there is no "claim" asserted by a third party — but instead focuses on the facts uncovered in the investigation. Certain facts that may be particularly important in assessing relatedness include commonalities in the vulnerabilities exploited, the attack vectors, information compromised, identity of the wrongdoers, and other similarities.

Insurers need to recognize the unique coverage considerations when assessing "related claims" issues under cyberpolicies. Unlike third-party claims, where the insurer and insured may very well be on a "level playing field" in assessing relatedness, relatedness in the first-party context is different because the insured is, at least in the first instance, in control of the relevant information.[2] Therefore, the insured may attempt to decide

what to disclose (or not to disclose) to its insurer. While an insurer can protect itself to a certain extent by incorporating cooperation requirements in its policies (and by including detailed requirements with respect to proofs of loss), an insured may elect to fight disclosing certain information to its insurer, or otherwise attempt to obscure relevant facts, if it believes doing so would help it avoid an unwanted coverage outcome. Insurers should vigorously avail themselves of the rights set forth in the policy terms the parties bargained for at the outset of the contracting relationship.

Given the potential asymmetry of information, insurers should carefully review and analyze information provided and follow up frequently in order to ensure that their rights are being adequately protected. Insurers at a minimum must ask the "right" questions — and make sure they get clear answers — when related claims issues may be presented. Insurers also may call upon forensic investigation experts — beyond the experts working directly with the insured — to advise them in connection with "related claims" issues.

The investigation of one data breach often leads to the discovery of another. As these investigations often take place over a limited time period, organizations may discover multiple data breaches (or multiple pieces of the same breach) in a short period of time. These situations require insurers and policyholders to carefully analyze "related claims" language and the specific facts and circumstances at issue. While there have been no reported decisions addressing related claims in the context of cyberinsurance policies, the law in other areas is well developed, and courts will likely look to those precedents for guidance in resolving complex coverage questions.

[1] Different policy forms accomplish this same general objective in different ways.

[2] In many jurisdictions, relatedness may focus solely on the language of the relevant policy and the language in the relevant pleadings. By contrast, some other jurisdictions may permit the introduction of extrinsic evidence to analyze relatedness.