MURTHA MEANS MORE INDUSTRY INSIGHT

The Connecticut Supreme Court Affirms Denial of CGL Coverage For Electronic Data Breaches

In a *per curiam* decision to be officially released on May 26, 2015, the Connecticut Supreme Court affirmed an Appellate Court decision denying insurance coverage for liabilities related to an electronic data breach. Although the case, Recall Total Information Management, Inc., v. Federal Ins. Co., SC19291 (May 26, 2015), may ultimately be limited to its rather unique facts, it stands as a stark reminder that general liability policies will provide coverage for electronic data breaches only in a limited number of circumstances. To properly protect your business, you should look to cyber security policies to obtain more fulsome coverage for these risks.

The Recall Case involved computer tapes containing the personal information of thousands of IBM employees, including social security numbers, that fell out of a truck onto a highway and ended up in the hands of an unknown person. IBM incurred more than $6 million in costs taking steps to prevent potential harm from the dissemination of this information and sought reimbursement of those sums from Recall Total Information Management, Inc. ("Recall"), which had contracted with IBM for vital records storage. The trucker, a subcontractor to Recall, had obtained commercial general liability ("CGL") and umbrella liability coverage from Federal Insurance Company and Scottsdale Insurance Company respectively, in which Recall was named as an additional insured. Recall and its trucker sued the insurers to obtain coverage for their defense and settlement of IBM's claim.

The Connecticut Supreme Court decision adopted the Appellate Court's opinion, AC No. 34716 (Jan. 14, 2014), which had construed two significant terms of the policy: the duty to defend and personal injury.

First, the Appellate Court concluded that the insurers had not breached their duty to defend. The negotiated settlement between IBM and Recall did not trigger the insurers' duty to defend, because no "suit" had been instituted. The policy defined "suit" as "a civil proceeding in which damages, to which this insurance applies are sought . . . [and] includes arbitration or other dispute resolution proceeding . . . to which the insured must submit or does submit with our consent." Based upon a plain reading of the policy, the Court could not conclude that "the term 'suit' or phrase 'other dispute resolution proceeding' was meant to encompass the mere negotiations that took place in this case." In reaching this conclusion, the Court noted that the policy's use of the terms "suit" and "claim" separately required that a distinct meaning be given to each. Additionally, the plain meaning of the term "other dispute resolution proceeding" could not be expansively interpreted to include informal discussions.

Next, the Appellate Court ruled that, because there was "nothing in the record suggesting that the information on the tapes was ever accessed by anyone," the loss was not covered under the personal injury provision of

If you have any questions about the issues addressed here, please feel free to contact a member of our Insurance Recovery Group:

Francis J. Brady
fbrady@murthalaw.com

George A. Dagon, Jr.
gdagon@murthalaw.com

Michael J. Donnelly
mdonnelly@murthalaw.com

Marilyn B. Fagelson
mfagelson@murthalaw.com

Melissa A. Federico
mfederico@murthalaw.com

David P. Friedman
dfriedman@murthalaw.com

Rachel Snow Kindseth
rkindseth@murthalaw.com

Elizabeth J. Stewart
estewart@murthalaw.com

Andrew G. Wailgum
awailgum@murthalaw.com

Kristen L. Zaehringer
kzaehringer@murthalaw.com

the policy. Although the policy covers injury "caused by an offense of … electronic, oral, written or other *publication* of material that … violates a person's right to privacy" (emphasis added in opinion), the Appellate Court concluded that there was insufficient proof of *publication* here. Without expressly adopting a precise definition of publication, the court held that "access is a necessary prerequisite to the communication or disclosure of personal information." Despite the fact that IBM had expended substantial sums to protect against identity theft, including restoring the credit of some of its employees, the parties had agreed that no identity theft incident could be traced to the loss of the IBM tapes. Unable to infer from the facts that publication had occurred, the Appellate Court concluded that the policyholder had not established coverage for personal injury under the policy.

The Appellate Court also rejected the policyholder's argument that the mere triggering of a notification statute creates "presumptive invasions of privacy" constituting personal injury under the policy. The data breach statutes require notification to potentially affected individuals, which can be a costly endeavor. However, these statutes do not provide for compensation from identity theft or the increased risk thereof and therefore the Appellate Court held that the mere triggering of a notification statute is not a substitute for personal injury.

Recall stands as a warning to policyholders of the costs and coverage issues associated with data security breaches. Its holding leads to the unfortunate result that CGL coverage may only be available ***after*** the lost data harm others. Recall is also a good reminder to review your current policies to ensure you have the proper coverage for your business. Historically, traditional CGL and property insurers did not respond well to claims of data breach and began adding specialized exclusions to preclude coverage. In the future, even this limited coverage is likely to be further reduced. New standard insurance forms to be issued by the Insurance Services Office later this year are expected to add electronic data breach exclusions to general liability policies.

Many, if not most, insurers now offer some form of cyber liability coverage as either a stand-alone insurance policy or an additional endorsement to an existing insurance program. There are three fundamental coverage types: liability for loss or breach of the data, remediation costs to respond to the breach, and coverage for fines and/or penalties imposed by law or regulation. Coverage can be triggered by failure to secure data; loss caused by an employee; acts by persons other than insureds; and loss resulting from the theft or disappearance of private property.

As the Recall case suggests, the cost of addressing a data breach can be significant. In 2014, NetDiligence reviewed 117 insurance claims submitted under cyber liability insurance policies between 2011 and 2013 and reported that hard costs (claim payout, crisis management and legal expense) associated with data breach claims averaged nearly $1.8 million. Click here for more information. Consult a broker with experience in cyber liability policies to find coverage appropriate for the risks that are specific to your business.

If you have questions with regard to the above, please contact Marilyn B. Fagelson at mfagelson@murthalaw.com or 203.772.7725 or Rachel Snow Kindseth at rkindseth@murthalaw.com or 203.772.7774.