Fine Print Online
October 2014

Securing Insurance for Cyberbreach Investigations

by Joshua Gold

As many directors and officers (D&O) insurance policyholders know, the costs of conducting and responding to an investigation are substantial—and that is definitely now true in the cyberbreach context. If there is a serious breach, the odds are overwhelming that the victim will incur enormous costs for the investigation process. Accordingly, insurance is often pivotal in addressing the impact to a policyholder for such expenses.

Cyberbreach investigation costs generally can be broken down into two categories. First, there are the internal costs of investigating and assessing the breach incident. This process often enlists several professional groups, including forensic computer specialists, in-house and outside counsel, and internal members of an entity's IT department. These costs are incurred to address multiple necessities: 1) finding out what was stolen and when; 2) figuring out if any other system vulnerabilities still exist; and 3) enabling the breach victim to adequately protect itself against the imminent onslaught of civil suits, investigations, inquiries from regulators and the like.

The second category of costs is comprised of those incurred to directly address inquiries and investigations from third parties, such as state attorney generals, the FTC, and potentially other regulators such as the SEC. With any significant breach, it is a sure bet that policyholders will be dealing with not one state attorney general, but several. Most significant breaches cross state lines and implicate state specific laws and regulations as a result, including compliance with notification requirements to affected state residents.

Thus, if you do business with individual consumers and obtain their personal identifying information (including for example, credit card information), it is advisable to obtain insurance coverage (including attorney fees coverage) for the inevitable expenses of responding to informal inquiries and formal proceedings that ensue from state attorney generals, the FTC and others when a breach occurs.

A word on those "others": it is not just the FTC that is taking a more active role in responding to cyber breach threats. Since 2010, the SEC and a consortium of bank regulators including the OCC, the Federal Reserve and the FDIC have all made formal pronouncements to those they regulate regarding cyber related risk. Policyholders can expect this increased interest to continue.

Policyholders facing the substantial costs of dealing with investigations may have insurance coverage to respond to and pay for all or a significant portion of these costs. Some of the specialty cyberinsurance products offered in more recent years promise to pay insurance coverage for such expenses. But beware, there is little uniformity of product presently and many of these cyberpolicies are vague and confusing for those attempting to divine the actual scope of insurance coverage the policies promise to provide. Policyholders are also wise to review their other commercial insurance policies. Business package policies, general liability policies, D&O insurance, E&O insurance and crime insurance policies may also provide a measure of protection against such costs depending upon their specific terms.

For example, in a recent case, a large retailer was able to secure crime insurance coverage for the costs of internal computer forensic costs, attorney fees and expenses incurred in dealing with an FTC inquiry under a Computer Fraud endorsement. This was despite the insurance company's repeated disclaimer of coverage and efforts to avoid providing it. As such, do not rule out the coverage that may be provided under other

insurance policies—even where those insurance policies are not dedicated cyber insurance policies.

Preserve Your Rights

When a cyberbreach occurs, policyholders must scramble to keep up with a very serious and also fluid set of challenges. Class actions may get filed within 24 hours of the incident being made public. Regulators will be contacting the breach victim quickly for information to determine whether consumers, residents or others have been affected. With all that is going on, insurance may be pushed to the back burner. Do not let this happen.

When a breach occurs, give notice under all potentially applicable insurance policies as early in the process as you can. There is no doubt that the meter will be running the minute the breach becomes known. Insurance companies dislike receiving bills for so-called "pre-tender" claim amounts. Because of this, it is very important to get notice in early and detail as best you can the identity of the computer and legal professionals you are using and what their costs are. This can go a long way to minimizing the number of disputes you will have with your insurance company in the face of a major cyberinsurance claim.

Given the ominous trend of cyberbreaches, be vigilant, be prepared, and don't forget during the ensuing mayhem to address the insurance coverage aspects promptly. ■

Joshua Gold, *a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.*

RISK MANAGEMENT