LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication • Novmeber 2012

Insurance Coverage for Data Breach Claims

By Richard D. Milone, Edward E. Weiman and Cameron R. Argetsinger

Data breaches caused by hackers or other forces outside the control of a business are a scary and expensive proposition for any organization that collects or retains personally identifiable information, or warehouses credit or financial information. According to a recent study by Symantec, an average data breach will cost an organization $5.5 million, including direct costs such as engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions, discounts for future products and services, and indirect costs such as in-house investigations and communication. See Symantec Corp. and Ponemon Inst., 2011 Cost of Data Breach Study, United States (2012). These costs are in addition to the costs of potential litigation (often in the form of a class action) by customers alleging that the company failed to take adequate measures to protect their data, and investigations by government agencies, such as the Federal Trade Commission (FTC), that frequently become involved when breaches affect a large number of consumers.

The risk of a data breach is not limited to financial institutions or businesses engaged exclusively in e-commerce. Any business that accepts credit cards as a form of payment, which includes practically every business on earth, is at risk. In fact, smaller-sized brick and mortar business are frequently targets of hackers who assume, rightly or wrongly, that such businesses lack the ability to detect and prevent theft of customer data.

Like any potentially catastrophic problem, insurance can be at least a partial solution. This article examines insurance coverage for data breaches. In-house counsel may be surprised to learn that coverage for data breaches is not limited to specialty policies, and can often be found under standard CGL or property insurance policies. Any time a potential data breach occurs, it is essential for an insured to consider all forms of insurance that it carries and to provide prompt notice to its insurer(s) of any policy that even potentially could apply.

CGL Coverage

Virtually all organizations carry some form of comprehensive general liability (sometimes referred to as "commercial general liability") (CGL) insurance. CGL policies can and often do provide coverage for a data breach. Any liability insurance claim generally turns on three variables. The first and foremost is the policy language. Many policies are written on the widely used Insurance Services Organization (ISO) forms, but some carriers use their own forms, or vary the ISO policy language with endorsements. Therefore, when reviewing caselaw, it is imperative to consider whether a particular case is evaluating the same policy language as in the policy under analysis. The second variable is the allegations and proof in the underlying lawsuit, *i.e.*, the claim against the insured. Third is the applicable state law on insurance coverage issues. More than any other area of law, insurance law varies from state to state. Thus, it is incumbent on policyholders to research the applicable law in the applicable jurisdiction when assessing and pursuing their claim.

For data breaches, coverage should be considered under "Coverage B" of a typical CGL policy, which provides coverage for "personal and advertising injuries." Whether data breaches are covered will usually depend on the policy's definition of a "personal and advertising injury." A standard ISO form defines that term as an "injury" arising out one of several different types of scenarios. The key scenario for data breach claims is usually defined as "oral or written publication, in any manner, of material that violates a person's right of privacy."

The two most frequently debated issues under CGL policies for data breach claims are whether the compromising of data: 1) constitutes the "publication" of that data; and 2) violates a "right of privacy." In a typical data breach case, a hacker will steal data from a policyholder's private network. Insurers often argue that this does not qualify as "publication" of that information, since it is not disclosed to other third parties. Likewise, carriers argue that the "right of privacy" simply means the right to be left alone rather than the right to keep private information protected.

There are not many decisions on these issues, but the few reported decisions are generally favorable to policyholders. For example, in *Netscape Communications Corp. v. Federal Ins. Co.*, 207 WL 2972924 (N.D. Cal.), aff'd in part, rev'd in part, 343 Fed. Appx. 271 (9th Cir. 2009), the Ninth Circuit found that Netscape was covered under the personal and advertising provision for lawsuits filed by its users claiming that Netscape's "Smart Download" program was acquiring data about Internet search histories without their knowledge. The court held that the users' claims met the "publication" prong, even though Netscape was not disclosing or publishing that information to third parties. The court also found that Netscape's harvesting of the users' private data met the "right-of-privacy" prong. One case that has not reached conclusion, but will undoubtedly have major implications for data breach insurance claims, is *Zurich American Insurance Co. et al. v. Sony Corp.* of America et al., currently pending in New York state court. In that case, Sony is

Richard D. Milone (rmilone@kelleydrye.com) is a partner and the chair of the insurance recovery practice of Kelley Drye & Warren LLP. Resident in the firm's Washington DC, office, Milone has represented commercial policyholders in all types of property and casualty coverage disputes. Edward E. Weiman (eweiman@kelleydrye.com) is a partner in the firm's Los Angeles office. He represents film and television companies and non-entertainment clients nationwide in intellectual property, entertainment, insurance recovery and general business litigation. Cameron R. Argetsinger (cargetsinger@kelleydrye.com) is an associate in the insurance recovery practice in the Washington, DC, office.

seeking coverage for a series of breaches of its PlayStation network, which exposed the personal information of some 77 million users. So far, 55 class actions have been filed against Sony, all of which have been consolidated into a single action. Zurich filed a preemptive lawsuit seeking a declaration that it has no obligation to cover Sony for the claim. While no rulings have been made to date, coverage attorneys are watching this case closely, as it will likely shape the law for coverage of data breaches.

Under a CGL policy, it is important for a policyholder to remember that it is not only required to notify its carrier when a lawsuit is filed; it must also provide notice when it first learns of an occurrence that might potentially lead to a lawsuit. This means that the policyholder must inform the carrier as soon as possible after a data breach occurs if that breach might lead to a claim from a third party, even before a suit has been filed or threatened. The policyholder's failure to do so is not necessarily fatal, but it provides ammunition for an insurer to deny the claim.

A private party's lawsuit is not the only type of claim that triggers coverage. Sometimes, CGL policies can provide coverage for FTC or other governmental agency proceedings. In those cases, coverage will often turn on whether the relief sought by the government can be interpreted as "damages" under the policy. Occasionally they can.

Finally, insurers are beginning to add specialized exclusions to CGL policies to preclude coverage for data breaches. A common example is titled a "breach of security" exclusion. When procuring insurance, policyholders at risk for data breaches should be cognizant of these exclusions and beware of what they are buying. Likewise, an insured who is able to bargain for a policy that does not have one of these exclusions has an excellent argument that its CGL policy does cover data breach risks, since the addition of an exclusion strongly implies that the policy itself, without the exclusion, must cover whatever the insurer is taking steps to exclude.

Property Insurance Coverage

First-party property insurance, another standard form of coverage, also provides a source of recovery for the costs that businesses incur in connection with data breaches. Property insurance generally covers direct physical damage to property. Thus, the critical question for a data breach claim is whether the compromising of electronic information constitutes direct physical damage. As with CGL coverage, state courts' interpretations of this language plays a significant factor in the outcome of any coverage dispute and (not surprisingly) vary from state to state. Fortunately, there is a growing body of case law that is favorable to policyholders in this regard.

In *NMS Services Inc. v. The Hartford,* 62 F. App'x 511 (4th Cir. 2003), the Fourth Circuit held that when a software company's former employee hacked into its network and erased vital computer files and databases, that constituted physical damage to property, even though the information only existed in electronic form. The concurring opinion in that case described the physical properties of electronic information as the rearrangement of atoms or molecules on a disk such that the erasure of that information constituted physical damage — a description that clearly recognizes the physical nature of what might otherwise seem like ephemeral electronic information.

In a similar case, *Landmark American Insurance Co. v. Gulf Coast Analytical Labs.*, Inc., No., 10-809, 2012 U.S. Dist LEXIS 45184 (M.D. La. Mar. 30, 2012), a policyholder sought coverage under a property insurance policy after it lost data on a hard drive storage system that had become corrupted. The insurer argued that because the hardware storing the data was not damaged — only the data had been lost — there was no direct physical damage. The court disagreed, holding that electronic data has physical existence and can be observed, altered or damaged through physical interaction.

Courts have even held that the loss of access to data can constitute physical damage for purposes of property insurance. In *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.,* No. 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000), a policyholder sought coverage after it lost access to electronically stored customer and product order information caused by a power outage that prevented it from performing its customer service functions. The carrier maintained that there was no coverage because the power outage did not damage any equipment. However, the court held that physical damage was not limited to physical destruction and could include loss of access or loss of use of data.

Coverage Under Other Standard Lines of Coverage

There may also be coverage under additional lines of insurance besides CGL and property insurance, and policyholders should err on the side of "over-noticing" when determining which insurers should be notified of a data breach. For example, coverage has been found under an errors and omissions (E&O) insurance policy when an individual sued an online marketing firm alleging that his computer crashed upon visiting the firm's website. *Eyeblaster, Inc. v. Fed. Ins. Co.,* 613 F.3d 797 (8th Cir. 2010). Coverage for data breaches has also been found under crime & fidelity insurance policies. *See Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA,* Case Nos. 10-4576/4608 (6th Cir. Aug. 23, 2012); *Scottrade, Inc. v. The St. Paul Mercury Ins. Co.,* No. 4:09-cv-01855-SNLJ (E.D. Mo. Nov. 12, 2009). In light of the wide range of policies that could respond to a data breach loss or claim, the primary rule for policyholders should be: when in doubt, tender.

Coverage Under Specialty Policies

Finally, policyholders who do not want to risk a dispute over whether a data breach claim falls within a CGL, property or other form of insurance coverage can purchase specialty policies designed specifically to protect against data breaches. A number of insurance carriers offer these policies, including ACE, AXIS, Chartis, Chubb, CNA, General Star, Travelers and others. These policies fall under a number of different headings (*e.g.*, "Security and Privacy Protection," "Cyber Security Liability," and "Network Security and Privacy Liability" to name a few). Common policy conditions include digital asset loss (*i.e.*, corruption or destruction of data due to security failure), cyber extortion coverage (*e.g.*, threats to release information or to introduce malicious code) and breach response (*i.e.,* crisis management). With any of these policies, which do not typically follow standard ISO forms, the devil is in the details. Policyholders must examine the terms and definitions of the policies closely to ensure that they are purchasing coverage commensurate with their risks.

Conclusion

The most important thing to know about insurance coverage for data breach claims is that it is available under the most commonly held forms of insurance: CGL and property insurance. In the event of a data breach, it is critical for policyholders to notify their carriers early and broadly, *i.e.*, to make sure that notice is given under any and all potentially applicable policies. Finally, given the state-specific nature of coverage law, policyholders should make sure they have a firm understanding of the applicable opinions in the relevant state when pursuing coverage for a claim.