



# INSURANCE COVERAGE FOR DATA BREACH CLAIMS

By Bruce A. Friedman, Esq.

Recent examples of data breaches resulting in invasion of privacy lawsuits abound. Target and other retailers, financial services companies and other businesses have had their internal data systems breached and consumers' private financial information stolen. There are insurance policies designed for such risks, but they are a relatively recent development. Yet, according to a recent article in the *Boston Globe*, only one-third of American businesses have purchased these new data breach policies. So what do the other two-thirds of the business community do when confronted with a data breach lawsuit?

In mediating both data breach disputes and insurance coverage cases arising out of similar claims, I have had to review and consider whether any insurance coverage applies to protect a business under these new circumstances. The most common policies held by businesses include comprehensive general liability (CGL) policies, directors and officers liability (D&O) policies and crime coverage, often included in fidelity policies.

CGL policies are the bedrock of commercial insurance and cover property damage and bodily injury claims. They also include coverage for various offenses, including invasion of privacy. Depending on the wording of the invasion of privacy offense, and absent an exclusion for Telephone Communications Privacy Act (TCPA) claims and the likelihood that new policies will reflect an exclusion for claims arising out of data breach (insurers generally exclude claims covered under policies that are written for specific risks), a CGL policy should cover invasion of privacy claims arising out of data breach. There are policies, for example, that provide coverage for "making known to any person or organization written or spoken material that violates an individual's right of privacy." This language would appear to provide coverage for data breaches, but according to the California Court of Appeal, it does not provide coverage for claims under the TCPA. In *ACS Systems, Inc. v. St. Paul Fire and Marine Ins. Co.*, the court found that the foregoing language violates the secrecy right of privacy, but not the seclusion right of privacy. Since most data breaches violate the secrecy right of privacy, coverage should be afforded under this language for invasion

of privacy claims arising out of data breaches, as those claims are based on the failure to maintain private personal information about the claimant. Violation of the seclusion prong of privacy, being free from unwanted intrusion, is not covered, according to the Court of Appeal, under language that requires that private information be made known to others.

D&O policies provide coverage for the directors and officers of a corporation, and possibly the corporation itself, for wrongful acts defined broadly to include acts, errors and omissions. Obviously, a claim for invasion of privacy arising out of a data breach would be based upon a contention that the entity did not take adequate steps (an omission) to protect its system from hacking, which resulted in the data breach and the dissemination of customers' private information. The catch, however, is that D&O policies have an exclusion for invasion of privacy claims. Insurers take a literal approach to the exclusion and argue that since the policy excludes invasion of privacy, then any claim based on an invasion of privacy, whether common law or statutory, is excluded. They rely on such cases as *Resource Bank v. Progressive Cas. Insurance Co.*, in which the district court applied the invasion of privacy claim to a TCPA class action, finding no coverage.

Policyholders respond based in part on the ACS Systems case, supra, that if invasion of privacy has both a secrecy and a seclusion prong, perhaps the exclusion is ambiguous and should be construed to provide coverage. This argument is coupled with the traditional coverage tenet that grants of coverage are to be construed broadly and exclusions are to be construed narrowly. So the argument goes that the invasion of privacy exclusion should be construed narrowly to apply only to one or the other of the prongs of the invasion of privacy offense depending on the nature of the claim being asserted in the underlying case.

Commercial crime policies may also provide coverage for losses resulting from data breaches. They often include computer fraud coverage for loss or damage to property resulting from the use of a computer to fraudulently transfer that property. This coverage is found in fidelity policies such as Banker's Blanket Bonds and

1.800.352.JAMS | [www.jamsadr.com](http://www.jamsadr.com)

*This article was originally published by LAW.COM  
and is reprinted with their permission.*



other crime policies issued to financial institutions and businesses. Insurers construe this policy to provide coverage for losses resulting from computer hacking, which is the source of the recent raft of data breach cases that we have seen in this country.

While obtaining insurance for claims arising out of data breaches is a good idea, most businesses have not purchased this insurance, but they may be the subject of a data breach resulting in individual or class action lawsuits. It is incumbent upon counsel to look for coverage under traditional insurance policies and to place the insurers on notice of the claims and involve them in the defense and settlement of the claims.

I have found that the presence of an insurer in the mediation of invasion of privacy claims makes it easier to settle the case. Adjustors have a depth of experience in actions of all types and can offer good insight on valuation and the structure of the settlement. Obviously, having insurance as a source of payment is helpful even in cases where the insurer is defending under a reservation of rights to deny coverage. Depending on the size and financial strength of the defendant business, the coverage issue may be used as a means of bringing the settlement value down if insurance is the only source of payment or recovery. ■

**Bruce A. Friedman, Esq.** is a JAMS neutral, based in Southern California. He is an accomplished dispute resolution professional who has mediated a wide range of disputes including insurance, class action, professional liability, business, real estate and entertainment matters. He can be reached at [bfriedman@jamsadr.com](mailto:bfriedman@jamsadr.com).