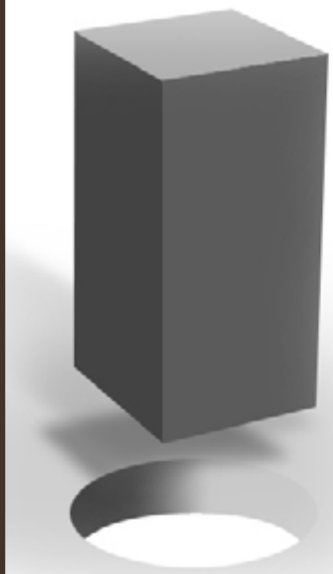

Data Loss Under CGL Policies:

The Proverbial Square Peg In A Round Hole

By Robert D. Laurie and Katherine A. Scanlon

Only a day after online shoe retailer Zappos notified 24 million customers of a data breach, a class action was filed against Zappos and parent company Amazon, alleging invasion of privacy and seeking damages, credit monitoring, and identity theft insurance. The filing of the lawsuit reflects a widely-held but erroneous belief that a breach of Internet security or loss of data is, per se, an actionable harm.

Indeed, several courts, have rejected such claims, and have concluded that the increased risk of identity theft is not actionable. Courts, including the U.S. District Court of the Southern District of New York in *Hammond v. Bank of N.Y. Mellon Corp.* (S.D.N.Y. Jun. 25, 2010), have acknowledged that the plaintiff must allege—and ultimately prove—an "injury in fact" that arose from the loss of data tapes containing personal information in order to assert a claim for violation of privacy rights. A year earlier, the court in *Randolph v. ING Life Ins. & Annuity Co.*, (D.C. 2009), reached the same conclusion, in a case involving a stolen laptop computer.

Nevertheless, it is an obvious reality that the Internet and technology have significantly transformed business, including the emergence of risks that threaten a company's bottom line. Indeed, in addition to the litigiousness that is reflected in claims like the one-day-old Zappos class action, states have enacted laws that often require, among other things, notification to all persons potentially impacted by a data loss or data security violation. The costs of complying with regulatory obligations alone could easily exceed millions of dollars. According to the Second Annual Cost of Cyber Crime Study by the Ponemon Institute, the cost of cyber-crime continues to rise, with a reported median annualized cost for 50 organizations to be $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company.

Unlike an advertisement fax sent to thousands of individuals, which some courts have construed as a "publication," a security breach involving the loss or theft of personal information is not a publication.

In addition to data loss or cyber-theft scenarios, businesses that maintain websites and include the Internet as part of their operating platform are exposed to a host of emerging liability issues. Disseminating information via a website may create liability risk not previously anticipated such as copyright infringement, defamation and invasion of privacy. Moreover, new legislation continues to create potential liabilities, particularly in the areas of user privacy and domain name infringement.

Despite the regulatory and liability risks involved, many businesses reportedly harbor misconceptions about cyber insurance and mistakenly believe that standard corporate insurance policies or general liability policies cover losses related to cyber liability. The reality is that traditional forms of risk transfer such as general liability insurance often do not apply to these emerging risks. Where businesses seek such coverage from general liability insurance, they do so with a square-peg-in-round-hole approach.

In a number of cases, businesses have sought insurance coverage for damages or consequential costs arising from a data loss or data security breach on the basis that such "damages" resulted from a "publication" that caused an "invasion of privacy" and thereby triggered the "personal injury and advertising injury" coverage within a general liability policy. That line of reasoning is not persuasive to insurers. For example, in the recently filed case *Colorado Casualty Ins. Co. v Perpetual Storage, Inc.*, the insurer seeks a declaratory judgment that a general liability policy and a commercial liability umbrella policy do not cover claims brought against its insured for liability arising from the loss of unencrypted back-up tapes.

These arguments typically give rise to a number of coverage questions, including whether data theft can constitute a "publication," whether consequential costs incurred as required by statute or regulation constitute "damages" and whether the mere loss of data alone constitutes a privacy violation unless there is evidence that a third party actually read the private data.

In demanding coverage relating to lost or stolen data, insureds often rely on case law from "blast fax" insurance coverage disputes. In "blast fax" cases, an insured allegedly faxed one advertisement to thousands of people in violation of the Telephone Consumer Protection Act. Several courts have ruled that coverage exists for insureds in a "blast fax" case because the act of sending a document to thousands constitutes a "publication" within the meaning of a general liability policy. One court that reached this conclusion was the Massachusetts Supreme Court in *Terra Nova Ins. Co., v. Fray-Witze*, where the court

Robert D. Laurie and Katherine A. Scanlon are litigation partners at the law firm of Seiger Gfeller Laurie LLP. The firm regularly represents insurers in complex insurance coverage determinations, counseling, litigation and extra-contractual disputes.

held that the transmission of 60,000 facsimile advertisements constituted a "publication" within the meaning of advertising injury coverage for oral or written publication of material that violated a person's right of privacy.

Courts have also considered whether such a "publication" actually invades the recipient's privacy, even though the content of the facsimile does not include a recipient's personal or private information. Several courts have reasoned that the person's receipt of a facsimile advertisement, in violation of the TCPA, violates the recipient's right of seclusion, rather than secrecy, and thus, constituted an invasion of privacy. Other courts, like the court in the case of *Cynosure, Inc. v. St. Paul Fire and Marine Ins. Co.* (1st Circuit, 2011), have ruled that the act of sending a facsimile advertisement, in violation of the TCPA, is not the act of "making known to any person or organization written or spoken material that violates a person's right of privacy."

Moreover, the "blast fax" insurance cases do not readily apply to a data loss or data breach scenario, such as the Zappos incident. Unlike an advertisement fax sent to thousands of individuals, which some courts have construed as a "publication," a security breach involving the loss or theft of personal information may not be construed as a "publication." For example, in January 2012, a Connecticut court in the case *Recall Total Information Management, Inc., et. al. v. Federal Ins. Co. et. al.*, ruled that coverage did not exist under a commercial general liability policy and an umbrella policy for significant notification and other remedial costs that resulted when unencrypted data tapes containing personal information fell from the back of a truck and were stolen.

With the emergence of cyber liability and associated risk, the insurance market has responded with various cyber liability products. Businesses must appreciate that traditional insurance products may leave them exposed to significant liability, as recent litigation demonstrates.

One thing is certain, as technology and "e-business" continues to evolve, so too will a company's liability risk and insurance needs. ■