



CONVERGING RISKS IN A DIGITAL ECONOMY:

COUNTRY CLUBS, HEALTH CLUBS, AND OTHER SPORTS/RECREATION CLUBS

This is one installment in a series of “White Papers” prepared by ThinkRisk Underwriting Agency discussing the converging media and technology-related risks faced by various industry segments. The White Papers provide real-world examples of these emerging exposures, and explore the insurance ramifications of these developments. This installment of the series discusses risks faced by country clubs, golf clubs, health clubs and other sports-and-recreation membership clubs.

Introduction to the convergence phenomenon: Digital technology is a powerful tool that has changed the way virtually all businesses and other organizations operate. Digital technology has unleashed corporate creativity and efficiency, leading to new products and services, new ways to manage and store data, and new ways to interact and communicate with constituencies. At the same time, digitization and the way it permits businesses to gather, create, distribute and store information and media content has altered the risks of doing business in a fundamental way, and exposes inadequacies in the current insurance response to these new risks. Here’s how this phenomenon affects golf courses, health clubs and other membership clubs.

Network security and data privacy

Digital technology makes gathering and storing data easier, creating opportunities for membership clubs to collect and store vast amounts of data, including information about members and their families but also data concerning employees, guests, visitors, vendors, contributors and many others. This data may include names, addresses, social security numbers, personal email addresses, medical information, and of course financial data. Many membership clubs store personal financial information in order to facilitate automated or recurring bill payment programs. In addition, many clubs have online stores or in-club pro shops, and therefore collect credit card or other personal financial information from customers.

The consequences of a security breach can be significant. In the event of a potential breach of security, state laws in most jurisdictions require the club to notify all potentially impacted persons of the breach, the cost of which can be astronomical. If the information is used in a way that is damaging, the club could face liability claims as well, for failing to protect the data by maintaining reasonable safeguards. In

addition, the club may face additional costs such as purchasing credit monitoring services, hiring a forensic team to determine the cause of the breach and take corrective measures, and in some cases hiring a public relations firm to help manage communications with members and other impacted persons and to repair damage to its reputation.

There have been many examples of data breaches involving membership clubs and other similar organizations, including those listed below. The nonprofit organization Privacy Rights Clearinghouse maintains a chronological listing of data breaches, which can be found at www.privacyrights.org.

- In 2008, a spreadsheet listing names and social security numbers of members of The Princeton University Tower Club was inadvertently attached to an email announcing a club event. The Tower Club had to take steps to protect 103 members whose data had been compromised.
- Also in 2008, Okemo Mountain Resort was a target of efforts to gain access to credit card data by infiltration of its computer network. The intruder gained potential access to sensitive data including cardholder names, account numbers and expiration dates. An expert in data security and forensics hired by Okemo to assist in the investigation discovered that its computer system was improperly accessed by an outside party for a 16-day period.
- In 2009, Texas Attorney General Greg Abbott charged an Edinburg fitness center with failing to adequately store and safeguard documents that contained customers' sensitive personal information. Under Texas's Identity Theft Enforcement and Protection Act, businesses are legally required to implement procedures that ensure customers' sensitive personal information – including Social Security, driver's license, and financial account numbers – is protected from unlawful use or disclosure.
- In August 2007, employees of Lifetime Fitness in Dallas discovered discarded customer records in easily accessible trash cans behind the Dallas business. Information that was discarded contained names, addresses, Social Security numbers, driver's license numbers and credit card information, as well as the date of birth of several children.

Content: Membership clubs are all about creating a unique culture and identity, and branding is integral to that process. As a result, trademarks and copyrights are among a club's most valuable assets, and clubs can be quite aggressive in protecting those assets against actual or perceived infringement, which could tarnish the club's goodwill and reputation. Indeed, the terms of use on the websites of many country clubs contain prominent notices warning against infringement of the club's intellectual property.

In addition, membership clubs communicate frequently with their members and other constituents, and regularly utilize technology to facilitate these communications. Most clubs have newsletters and websites, which are likely to contain photographs, chat rooms, and other such content. Many clubs have Facebook pages, Twitter accounts and utilize other social networking tools to reach out to existing and prospective members. Many clubs frequently engage in local advertising, and host tournaments and other special events that may involve special appearances by athletes, celebrities or other

endorsers. All of these activities give rise to content liability exposures, similar to those faced by media companies and ad agencies, such as copyright, trademark and commercial misappropriation.

As a result, there are many examples of media and intellectual property claims involving membership clubs, including the following:

- The aptly named Due Process Stable golf club in Monmouth County, NJ, sued rival Eagle Oaks Golf Club, 10 miles to the south, in 2004 for trademark infringement. The dispute involved a pair of circular logos. The Due Process logo includes a horse head and a clover leaf. The Eagle Oaks logo includes a bald eagle head and an oak leaf. Due Process, which views itself as one of the most exclusive clubs in the state, alleged that the logo was causing confusion and tarnishing its good will.
- A Myrtle Beach, SC country club became embroiled in trademark litigation in Federal District Court with Ralph Lauren over the use of the club's emblem on shirts, jackets and other apparel. Ralph Lauren has been very active in litigating trademark claims. In 2005, it sued the United States Polo Association for infringement in connection with the Association's use of the famous polo player's emblem.
- In 1998, the Greenbrier Resort Hotel sued the Chesapeake Country Club over the use of the "Greenbrier" trademark and a stylized "G" emblem.
- Famed golf resort Pinehurst LLC, which is known for closely protecting the use of its name, filed a trademark lawsuit in 2007 in Federal Court against Legacy Golf Links in Aberdeen, GA. Pinehurst claimed that Legacy's Golf Links' pro shop has sold merchandise such as clothing and sporting goods that have the "Pinehurst" trademark on them

Coverages in the standard insurance marketplace

Although most membership clubs purchase Commercial General Liability ("CGL") coverage, typical CGL policies provide limited coverage for media and network security claims. Data breaches, and the attendant costs and claims associated with such breaches, are generally outside the scope of the GCL. Nor are the losses likely to be covered by a standard property policy, which generally requires physical loss or damage. With respect to content, libel and invasion of privacy in publications may be covered by the CGL, but that leaves much media activity unprotected. For instance, intellectual property is excluded under most newer versions of the CGL, except for limited coverage for copyright in "advertisements," which is strictly defined. This means that the litany of trademark and related intellectual property claims discussed above would likely not be covered. Website content is generally not covered, unless the content is considered "advertising," which is construed narrowly. Similarly, many D&O policies have intellectual property and other similar exclusions that would defeat coverage in many of the high-exposure areas discussed in this paper. Even when such coverage is provided, it is generally not robust, and the carrier may not have the necessary legal expertise to deal with highly specialized or technical claims.

ThinkRisk's Converging Risk Liability Policy: The Converging Risk Liability Policy from ThinkRisk addresses these unique and emerging exposures, and fills the gaps left by traditional policies. The policy

is “modular” and can therefore be customized to meet the needs of the particular club. Coverage Part A of the Policy provides coverage for claims arising out of the distribution of content, whether by print, electronic or any other means, including social networking. To the extent that the club provides any type of professional service, Coverage Part B can provide coverage for claims alleging errors and omissions in the course of providing such services. Coverage Parts C and D provide network security coverage, both for liability claims brought against the club (Part C), as well as for certain costs incurred by the institution in responding to a breach (Part D), such as the cost of notifying impacted persons and retaining a public relations consultant.

To obtain a quote, please contact your insurance agent. For more information, contact us at info@thinkriskins.com or (816) 994-6400.

