



CONVERGING RISKS IN A DIGITAL ECONOMY: RETAILERS AND E-TAILERS

This is one installment in a series of “White Papers” prepared by ThinkRisk Underwriting Agency discussing the converging risks faced by various industry segments as a result of the digital economy. The white papers provide real-world examples of such risks, and explore the insurance ramifications of these emerging exposures. This installment of the series discusses risks faced by traditional retail stores and their online counterparts, e-tailers.

Introduction to the convergence phenomenon: Digital technology is a powerful tool that has changed the way businesses and other organizations operate. Digital technology has unleashed corporate creativity, leading to new products, 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 companies 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 retailers and e-tailers.

Content: Whether a company sells goods from a traditional “brick and mortar” store or online from a website or (as in most cases) from both, retail companies are relying increasingly on media content to inform consumers and build loyalties. That content can range from traditional to cutting edge (including advertising, labels, websites, blogs, newsletters and even games) but all of it carries all the exposures of any media outlet. For instance, as with any media content, copyright and trademark infringement can arise from the unlicensed use of music, artwork, copy, slogans or any other expressive element. The desirability of many products can be enhanced if used by celebrities, but making that connection without the celebrity’s consent can lead to a misappropriation claim.

Some retail stores go beyond product information and seek to build loyalty and identification. Retail marketers try to connect consumers to particular brands with tools like travel guides, charitable organizations and home improvement classes. The message can be multi-dimensional, seeking to connect a brand with attractive lifestyles. For instance, rugged but fashionable apparel is often featured

in television programs about travel, fitness and other subjects and various tools are highlighted in home improvement shows. Much of that content comes from the retail product industry.

There are many examples of media and intellectual property claims involving retail sales both on and off-line:

- On October 1, 2010, Michael's Stores, Inc., the Texas-based chain of craft stores, was sued for copyright infringement by a Pennsylvania jewelry designer who claims that Michaels is selling ceramic charms that are knockoffs of her copyrighted designs.
- In June of 2010, Forever 21, a clothing and accessories retailer, sued Forever 26 for various trademark related infringements based on the similarity of the names.
- Paris Hilton sued Hallmark Cards in 2009, alleging misappropriation of publicity and trademark infringement for the use of her image and catchphrase on a birthday card.
- In 2009, a small electronics retailer called Sellify sued e-tail giant Amazon for trademark infringement and defamation over Google search ads that allegedly paint Sellify as a "scam artist."
- Amazon was sued again, along with one of its sellers, Shokomoko, in December of 2010 by Mint, Inc. alleging copyright, design patent, trademark and trade dress infringement for the sale of "hugging" salt and pepper shakers.
- In 1996, the Yankee Candle Company sued the New England Candle Company for copyright and trademark infringement based on the similarity of the design of the retail store itself.
- Larry Leigh, owner of Leigh's and Mettie's women's clothing stores in Grand Rapids, MI, was sued by ASCAP for playing tapes and CDs in his stores in violation of copyright regulations. The suit requested \$400,000 in damages.

False Advertising

Closely related to the issue of intellectual property in content, retail stores face a multitude of exposures relating to false advertising or misrepresentation in advertising. A store's advertising often contains representations as to the quality and origin of the product or its manufacturing – which may draw consumer or competitor complaints, especially when comparing products with competing companies. In an increasingly consumer-conscious society, consumer groups and government regulators are ever vigilant in identifying representations that they believe to be false or misleading, and bringing claims against the advertisers. These claims can be extraordinarily expensive to defend. Some examples of recent false advertising claims in the retail/e-tail market include:

- In November of 2010, seven California counties filed suit against Overstock.com, alleging that the online retailer, which claims to offer brand-name merchandise at discount prices, has made untrue and misleading claims about the prices of its products.
- Also in November of 2010, a putative class action lawsuit was filed against Target Corporation for fraud, false advertising and a number of other charges by a consumer who claims she was shortchanged on coupons.
- Saks Incorporated recently settled a lawsuit alleging that Saks Fifth Avenue and others have repeatedly engaged in false advertising and mislabeling of fur garments.

Network security and data privacy

Like many other businesses, retail stores are taking advantage of digital technology to learn more about their customers and stay connected to them. Often, that means gathering and holding private information about consumers collected through the business's websites and internet activities. In other settings, data may be collected in person, such as through point of sale store loyalty cards. Of course, retailers that take credit card or other payment information are now more aware than ever of the value and risks associated therewith. In addition, all businesses maintain data about their employees and former employees. This data, often referred to as personally identifiable information or PII, can be a powerful business tool, but carries with it the responsibility of protecting the information from unauthorized access or accidental disclosure.

In the event of a potential breach of security, state laws in most jurisdictions require the company 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 company could face liability claims as well. Despite these risks, a company's data security practices may not be state-of-the-art, because the company may lack the resources to hire full-time technology officers or to purchase top-of-the-line commercially available security systems.

There are many examples of data breaches involving interaction with consumers or involving employees. Many breaches are the result of intrusions from hackers and thieves, but the simple loss of a laptop (or other low tech act) is a frequent cause of breaches, too. Some breaches in the retail sales industry include:

- In 2010, debit card terminals inside or near ALDI grocery stores in an 11 state area were outfitted with skimming devices, allowing data thieves to gather customer credit card information at the point of sale.
- On August 30, 2010 a computer with customer information was stolen from SanDiegoFit.com, an exercise clothing e-tailer. The computer contained customer names, addresses, phone numbers and credit card numbers.
- In August of 2010, applications and resumes received by the discount clothing retailer, Ross, were found in a public dumpster. The applications dated back to 2002 and contained names, social security numbers and other contact information.
- In one of the largest and most-publicized data breaches ever, retail clothing outlet giant TJX, the parent company of T.J. Maxx and Marshall stores, disclosed in January 2007 that its systems were hacked, exposing over 94 million credit and debit cards to possible fraud. The direct costs of this breach are estimated to exceed \$5 billion.

Coverages in the standard insurance marketplace

Although most businesses purchase Commercial General Liability ("CGL") coverage, typical CGL policies provide limited coverage for media and network security claims. Libel and invasion of privacy in publications may be covered, but that leaves much media activity unprotected. For instance, intellectual property is typically excluded, except for copyright in "advertisements", which is narrowly defined. The result is coverage only for copyright infringement claims from "advertisements" placed in media such as newspapers and broadcasts, while trademark and other intellectual property

infringements (and copyrights claims outside of “advertising”) will not be covered. Similarly, website content is generally not covered, unless the content is considered “advertising.” Chat rooms, bulletin boards and other interactive media are excluded. Data breaches are also outside the scope of the CGL policy. 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.

False advertising claims are typically excluded from all types of policies.

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 institution. Coverage Part A of the Policy provides comprehensive coverage for claims arising out of the distribution of content, whether by print, electronic or any other means. Of particular importance to the retail and e-tail sales industry (because of representations made in advertising), Coverage A can be endorsed to cover false advertising claims. To the extent that the institution provides any type of professional service, Coverage Part B provides 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 institution (Part C) and for certain costs incurred by the institution in responding to a breach (Part D), such as the cost of notifying impacted persons.

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