ANDERSON KILL
POLICYHOLDER

September 2015

ALERT

FTC v. Wyndham Decision Highlights Need for Robust Cyber-Insurance Policies

By Robert D. Chesler

FTC v. Wyndham

Every company entrusted with any personal data at all must read the decision in *Federal Trade Commission v. Wyndham Worldwide Corp.*, No. 14-3514 (3rd Cir. Aug. 24, 2015). The court ruled in favor of the FTC and, among other findings, held that a company's publicly published privacy policy must match its actual practices. If the actual practices are inferior to the privacy policy, the company can be subject to an FTC investigation and enforcement action, and possibly to a class action. Wyndham's privacy policy stated,

> we safeguard our Customer's personally identifiable information by using industry standard practices … This [Wyndham's practices] protects confidential information … from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain "firewalls" and other appropriate safeguards. …

The FTC asserted that "the privacy policy on [Wyndham's website] … overstates the company's cybersecurity."

The decision in Wyndham arose in the context of a hotel chain, with many franchised hotels connected to a single Wyndham computer network. The court reasoned that a potential client might read the Wyndham privacy policy on line, think that Wyndham had a robust policy, and then be surprised that Wyndham's actual privacy safeguards did not measure up to its public statement. The Third Circuit found that misleading clients in this way would be "unfair," as set forth in the governing statute. 15 U.S.C. sec. 45(a). It is noteworthy that neither the FTC nor the Third Circuit contended that anyone did read the Wyndham privacy policy and use the hotel because they were misled by it. However, the court found that "A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on the promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."

Also, the FTC's list of Wyndham's alleged shortcomings demonstrates that the FTC will carefully scrutinize a company's data protection. The FTC identified seven specific areas where Wyndham's efforts fell short, including "easily guessable passwords," lack of firewalls, lack of adequate information, security policies and the failure to "adequately restrict the

ANDERSON KILL
1251 Avenue of the Americas
New York, NY 10020
(212) 278-1000 Fax: (212) 278-1733

ANDERSON KILL
864 East Santa Clara Street
Ventura, CA 93001
(805) 288-1300 Fax: (805) 288-1301

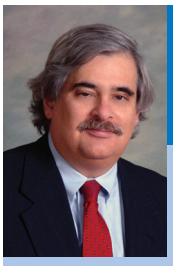
ANDERSON KILL
1600 Market Street, Suite 2500
Philadelphia, PA 19103
(267) 216-2700 Fax: (215) 568-4573

ANDERSON KILL
1055 Washington Boulevard, Suite 510
Stamford, CT 06901
(203) 388-7950 Fax: (203) 388-0750

ANDERSON KILL
1717 Pennsylvania Avenue, Suite 200
Washington, DC 20006
(202) 416-6500 Fax: (202) 416-6555

ANDERSON KILL
One Gateway Center, Suite 1510
Newark, NJ 07102
(973) 642-5858 Fax: (973) 621-6361

www.andersonkill.com



who's who

Robert D. Chesler is a shareholder in Anderson Kill's Newark office. Mr. Chesler represents policyholders in a broad variety of coverage claims and advises companies with respect to their insurance programs.
rchesler@andersonkill.com
(973) 642-5864

access of third party vendors to its network. …" These allegations are broad enough to likely sweep in the practices of many companies. (The Third Circuit's decision also addressed whether Wyndham had received fair notice, but this article does not address that issue.)

Moreover, while the FTC governing statute does not create a private cause of action, there is a danger that an enforcement action by the FTC could provide fuel for a class action against not only the company but also, potentially, its directors and officers. Plus, many state's consumer fraud acts are modeled on this statutory language, and certain of these acts do create private causes of action.

One essential takeaway from Wyndham's dispute with the FTC is that due care should be taken to ensure that the data protection system actually does match up to the company's public promises and disclosures. Moreover, if the company declares that its privacy system is "state of the art," the company must realize that "state of the art" is a moving target. Technology is rapidly evolving, as are the hackers' skills to thwart even the most sophisticated security systems.

Will Traditional Insurance Policies Provide Protection?

The next place for a company to look for protection is to its insurance program. Traditional policies may provide some relief. The general liability policy, in its personal and advertising injury section, provides coverage for invasion of privacy, which has already led to litigation over coverage for data breach claims. Cyber-related claims might also lead to claims of bodily injury and property damage. However, many general liability policies are now imposing exclusions (varying in scope) for any claim arising from cyber acts. While the general liability policy may not always provide coverage, it may still be effective against common law causes of action. In *Hartford Cas. Ins. Co. v. Corcino & Assoc.*, 2013 U.S. Dist. Lexis 152836 (Cal. Dist. Ct. App. Oct. 7, 2013), for example, a company was sued for data breach, and sought coverage under its general liability policy. The court found that since the company could also be liable under California's broad cause of action for invasion of privacy, the insurance company had to defend.

Broad D&O policies are also essential. An FTC investigation can easily produce a class action against a company's directors and officers. There is no reason why the D&O policy should not cover such a suit. Companies must be ever-vigilant against an insurance company adding a new exclusion or condition that impinges on this coverage.

Should I Purchase a Cyber-Insurance Policy?

This brings us to the latest insurance product, the cyber insurance policy, purportedly designed specifically for these cyber threats. These policies, in one form or another, have been around since about 2000, getting their start with the Y2K hysteria. At first they did not sell well at all, but in recent years sales have accelerated. In the early years, only companies that were viewed as a direct target, such as banks and health care companies, purchased these policies. However, every company is now a target. It is symptomatic that Beazley Insurance, a major player in this field, has offered the Beazley Breach Response

policy to professionals with small practices — CPA's with up to $5,000,000 in revenue and law firms with not more than 10 members. Beazley must think that even sole practitioners are so threatened by data breach risks that they will purchase a cyber-insurance policy.

What should a company look for when purchasing a cyber-insurance policy? Companies should be forewarned that the cyber-insurance market is like the Wild West. Insurance companies have not gathered together and produced a standardized policy. Every policy is different, often in critical ways, and insurance brokers can typically request specifically tailored cyber-policy terms. A company needs a cyber-insurance specialist, whether broker or consultant, when purchasing a cyber-insurance policy.

What should a company look for when purchasing a cyber-insurance policy? The list is endless. We have set forth below some key issues.

1. Does the policy provide coverage for government investigations, responses to subpoenas, proceedings, inquiries and other forms of actions, whether punitive or not, by government agencies and law enforcement?
2. Relatedly, does the policy exclude governmental fines and penalties? How does the policy define these terms? Under one policy, for example, the term "damages" does not include "criminal, civil, administrative or regulatory relief, fines or penalties."
3. Does the policy provide a crisis management fund? This is a coverage part that provides funds and expertise to assist the policyholder in responding to a breach and complying with legal notice requirements, for example setting up call centers.
4. What is the policy's retroactive date? A policy does not always provide coverage for acts that take place prior to the retroactive date, and many insurance companies use the policy's inception date as a "retroactive" date to dispute insurance coverage.
5. What policy limits do you need, and what deductible can you bear? Many companies see cyber insurance as catastrophic coverage, and use large deductibles. Others see it more as a controllable risk that needs only a small deductible.
6. One key issue is the definition of "claim" or "occurrence." Most cyber policies will have a deductible. If each separate wrongful act or claimant or instance of data breach is a separate occurrence or claim, the deductible could devour the coverage. The policyholder needs a limit on the application of deductibles.
7. Check out carefully, in particular, the policy's exclusions. Is there an exclusion that, if applied in a hyperliteral manner, guts the policy's protection? Are the exclusions overly broad or ambiguous?
8. Make certain that the insurance policy matches your particular needs. Different companies face different perils.
9. Make sure that your cyber policy provides coverage for claims involving in some way your vendors, including cloud providers and subcontractors.

10. Recently, Columbia Casualty Co. sued its client Cottage Health System in a cyber-insurance dispute. The policy had a provision "for failure to follow minimum required practices," as set forth in the insurance application. This condition is a recipe for a dispute with your cyber-insurance company.
11. How is "war" defined? War is often an excluded peril that is defined differently in different policies. The exclusion can be defined to include "acts of war and terrorism." Do these exclusions apply to hacking by a foreign government? In these perilous times, it is critical to have the narrowest possible definition of war.
12. In the fast-evolving cyber world, it is predictable that cyber-insurance policies may soon be out of date. A company needs to continually compare its exposures with its insurance policy's protections.

Conclusion

There is a nearly infinite array of issues involved in purchasing cyber insurance. If relying on cyber insurance, work with a seasoned broker to purchase the best protection you can. For many years, no reported cases existed of cyber-insurance coverage litigation and, anecdotally, insurance companies resolved the great majority of these claims without a public dispute. However, an insurance company and a policyholder have each recently filed litigation in open court. See *Columbia Casualty v. Cottage Health System*, Case No. 2:15-cv-03432 (D.Cal.); *Incomm Holdings, Inc. v. Great American Ins. Co.*, (D. Ga.). Everyone will have to wait to see if these are ripples in the water or the coming of a tidal wave.