# Cybersecurity Lessons From the Third Circuit's 'Wyndham' Ruling

Christopher M. Brubaker

September 16, 2015

In a much-anticipated decision, the U.S. Court of Appeals for the Third Circuit recently upheld the Federal Trade Commission's ability to regulate cybersecurity as an unfair business practice, in *Federal Trade Commission v. Wyndham Worldwide*, No. 14-3514, __ F.3d __ (3d Cir. Aug. 24, 2015). While the outcome is not necessarily a surprise given the facts of the case, the decision will carry significant implications for companies that collect and maintain consumer information. A potential caveat is whether Wyndham Worldwide Corp. seeks and is granted certiorari by the U.S. Supreme Court. Even if certiorari is granted, it would be wise to heed the lessons of this case while waiting on final word from the Supreme Court.

The FTC sued Wyndham Worldwide and three affiliated companies in federal district court for both unfair and deceptive business practices seeking injunctive and other equitable relief including restitution to consumers under the Federal Trade Commission Act, 15 U.S.C. Section 45(a). The FTC alleges that Wyndham failed to maintain reasonable and appropriate data security for consumer information in connection with a series of three data breaches in 2008 and 2009. More specifically, the FTC alleges that all three breaches took advantage of the same shortcomings in Wyndham's network, including storage of payment card information as readable text (failure to encrypt), allowance of "default" and easy-to-guess passwords, failure to use firewalls and other commercially available methods for protecting data, failure to ensure that hotels connecting to the network had adequate information policies and procedures, failure to properly restrict third-party vendor access to the network, failure to monitor for unauthorized access, and failure to follow proper breach response protocols. The complaint also alleges that the second breach utilized malware used in the first breach that had not been removed from the system and throughout the relevant time period Wyndham advertised that it used "industry standard practices" to safeguard customer information, including encryption and firewalls. The FTC also alleges that across the three breaches, the hackers downloaded personal and financial information for hundreds of thousands of consumers, which resulted in over $10.6 million in fraudulent charges.

Wyndham responded to the complaint by filing a Rule 12(b)(6) motion to dismiss, challenging both the FTC's ability to bring claims related to cybersecurity and whether those claims were properly pleaded. The district court denied Wyndham's motion, finding that the FTC had both the authority to act and had properly pleaded claims for unfair and deceptive practices related to Wyndham's cybersecurity under the act. The case was before the Third Circuit on an interlocutory appeal involving only the district court's decision upholding the FTC's ability to regulate cybersecurity as an unfair

business practice. Accordingly, the operative "facts" are the allegations made by the FTC in its complaint, which are summarized above.

The issues certified on appeal were whether the FTC has authority to regulate cybersecurity as an unfair business practice under the act and, if so, whether Wyndham had fair notice that its cybersecurity practices could fall short of the requisite standard. The standard for unfair conduct has been codified in Section 45(n) of the act, and requires substantial injury to consumers that is not reasonably avoidable by consumers and is not outweighed by any benefits to consumers or competition. Wyndham's main arguments about the regulation of cybersecurity were that there are additional requirements to bring a claim for unfair conduct beyond the standards in the act and that the act did not give the FTC authority to regulate cybersecurity. With respect to fair notice, Wyndham argued that it was entitled to know with "ascertainable certainty" what cybersecurity standards it was required to meet. While the court rejected all of these arguments, there are two aspects of the decision that warrant particular attention in terms of developing and implementing a cybersecurity program.

First, while the court acknowledged that the act did not expressly preclude additional requirements necessary to sustain an unfairness claim, it stated Wyndham's arguments in this regard were unpersuasive, while pointing out the lack of precedent or other authority supporting Wyndham's position. But the court went on to state that even if something more than the standards set forth in Section 45(n) was required, the conduct alleged by the FTC clearly satisfied any such additional requirements. In particular, the court pointed to the allegations regarding Wyndham's stated privacy policy and its failure to meet that standard, which the court viewed as deceptive conduct. The court noted that "deceptive" conduct is a subset of "unfair" conduct, and that while not all unfair activity is deceptive, all deceptive conduct is unfair.

Second, the court found that the "ascertainable certainty" notice standard was inapplicable here because, as Wyndham argued, there was no agency action (regulation, decision or adjudication) to apply the standard to. That is, parties are entitled to ascertainable certainty with respect to agency interpretation of statutes because they are not bound by the same interpretive constraints as courts. But when the court acts in the first instance to interpret the statute, as the court found was the proper approach here, the applicable standard was whether Wyndham had fair notice as to what the act required. The court characterized the notice required in this context as relatively low because no constitutional rights are implicated and the statute regulates economic activity. The court described the requirements of Section 45(n) as a cost-benefit analysis that, while not precise, was more than sufficient to meet the minimal notice requirements under the facts alleged in this case (failure to encrypt data, failure to use firewalls, failure to require default passwords to be changed, multiple breaches) because Wyndham could have reasonably foreseen that its conduct could be construed by a court as falling within the meaning of the statute. The court also referenced material published on the FTC's website, including a guidebook on protecting personal information and prior complaints filed by the FTC against other companies for cybersecurity issues as providing notice of what activities the FTC

viewed as failing to satisfy the requirements of the act. The court did not address Wyndham's arguments regarding "substantial injury," finding they were not within the scope of the interlocutory appeal. Thus, even if the Third Circuit's decision is not appealed, there are issues related to the FTC's ability to regulate cybersecurity under the act that could be addressed in further proceedings in this case.

Even though this may not be the last word on this ruling, there are two important takeaways from the decision beyond the obvious reminder to make sure your products and services live up to your advertising.

Stay vigilant and be proactive. A risk-management-based approach to cybersecurity has been the standard for some time. In an area where there are no surefire technological or product-based solutions, it is necessary to be proactive to stay ahead of the cybersecurity curve. Even the best cybersecurity program will quickly become obsolete without constant monitoring and adjustment. The threat is a fluid and evolving one that can lay dormant for months waiting for one wrong click to spring into action. This also means there is no secret recipe or magical formula for developing a cybersecurity program.

Designing the right cybersecurity program for your company requires understanding a plethora of information, including the ways in which you are at risk, the data or information that needs to be protected, the statutory and regulatory framework applicable to you, the technological solutions that are available, as well as the budgetary and human resources that are available to apply to the solution. The goal is to balance and utilize the available tools and resources to make your company as unattractive a target as possible. As the headlines will attest, mistakes can and do happen. When several mistakes happen in tandem, the results can be catastrophic. A proactive cybersecurity program is more likely to keep one mistake from turning into a series of mistakes and will allow your company to learn from others' failures.

This brings us to the second lesson: Make sure you have adequate insurance to protect your needs. Like cyberrisk, cyberinsurance is evolving. There are no uniform policy forms. The available coverage can vary widely in scope of coverage, amount or limits of coverage and cost from company to company. There is often flexibility in the coverage available and terms may be negotiated. Cyberexclusions are becoming more prominent in general liability and directors' and officers' policies, making it unwise to assume there is coverage for cyberevents in non-cyber-specific policies. Underwriting for cyberinsurance is largely predicated on a risk-management assessment of a company's cybersecurity program and can even involve a full-scale audit of the cybersecurity program. This process in and of itself can be helpful in evaluating your cybersecurity program and gaining additional insight about the current best practices. Even the best cybersecurity program is no guarantee that you will not be breached. But it should mean you have the proper insurance coverage in place to protect your company and keep it from facing charges from the FTC regarding "unfair" business practices.

***Christopher M. Brubaker*** *is an associate in Clark Hill's insurance and reinsurance practice group and concentrates his practice in commercial litigation, including appellate work. He also advises companies on regulatory matters involving insurance and environmental laws, rules and regulations. He can be reached at cbrubaker@clarkhill.com.*



203302321.1 09999/09998-1816