Enforcement

Views on Implications of the Wyndham Settlement With the FTC
From Chris Jay Hoofnagle, University of California, Berkeley

Hotelier Wyndham Hotels & Resorts LLC recently agreed to settle Federal Trade Commission charges (14 PVLR 2228, 12/14/15), bringing to an end what had been one of the most followed privacy and data security cases in years.

Bloomberg BNA Privacy & Data Security News Managing Editor Donald G. Aplin posed a series of questions to Chris Jay Hoofnagle, of the University of California, Berkeley, and a member of the advisory board of Bloomberg BNA's Privacy & Data Security Law Report on what the settlement means for companies facing FTC data security compliance and enforcement issues.

BLOOMBERG BNA: Were you surprised that Wyndham settled to end the FTC enforcement action?

Chris Hoofnagle: It made sense for both parties to settle. The FTC scored a significant win in the Third Circuit’s decision upholding the agency’s power to use its authority to address new threats to consumers (14 PVLR 1592, 9/7/15). That decision was in a way a no-brainer—the FTC’s flexible mandate is a feature that has allowed the agency to pivot from policing print, radio, television and then Internet-based practices over the decades without new authorities from Congress. On the other hand, if the FTC continued the case, it would have to prove the elements of unfairness at trial. Wyndham had signaled that the FTC’s facts would unravel. Additionally, the FTC could get most of what it wanted while avoiding trial risk through settlement.

Perhaps the settlement was surprising because of the intense, anti-administrative-state rhetoric that accompanied the Wyndham challenge. Both Wyndham and LabMD supporters seemed to be campaigning for a return to 19th Century consumer protection approaches. Why end this campaign? Well, I see such arguments as instrumental because the implications of rolling back the authorities of the FTC are counterproductive for the business community. If the FTC were required to promulgate a security rule, we would have years of battles resulting in a rule similar to Gramm-Leach-Bliley: a two-page-long exhortation to have “reasonable” secu-
The FTC's order makes it clear that Wyndham loses the benefits of having a clean assessment if it makes misrepresentations or if it makes material changes to its technical setup. These are meaningful, easy to violate exceptions. Because there is no mens rea attached to a misrepresentation, presumably any misrepresentation, including one made accidently, would suffice. Also, companies do change their architecture in order to game assessments. We see in PCI-DSS over and over again that companies are certified as PCI-DSS compliant, but then a breach happens and a post-breach analysis shows non-compliance.

The presumption of data security compliance if Wyndham obtains a clean PCI-DSS assessment is important because it is in effect a safe harbor from civil penalty/contempt actions. The FTC will have to go to court and overcome that presumption.

On the other hand, the PCI approach is a snapshot in time of compliance. The assessments, for all their warts, concern the operation of privacy and security programs over a long period of time. Thus, PCI is a more definite and objective standard, but it only deals with the narrow issue of card security, and only at one moment in time.

I think the next case to pay attention to is LifeLock, especially for those concerned that FTC actions do not afford adequate due process. Unfortunately, the case is sealed. But publicly-available information suggests that the case deals with information security. LifeLock publicly responded to the case by stating that it hired high-quality assessors to evaluate the company, that LifeLock spent millions to ensure compliance with the order, and that “[e]very audit completed by those third parties affirmed that we were in compliance.” Nonetheless, LifeLock has set aside over $100M to settle the case. Those who say they are concerned about FTC actions do not have to worry about a precedent-setting fine.

Does the Payment Card Industry Data Security Standard assessment to demonstrate compliance in essence provide Wyndham a safe harbor?

The FTC's original complaint conceives of injury as an intrusion into the credit card network. But the security problems alleged could have led to other invasions of privacy, such as release of customer transactional information. Wyndham's lawyers stopped the Commission from fencing in other kinds of privacy and security invasions.

The FTC's approach is different and is a mixed bag for the Commission. On one hand, the changes demonstrate that the Commission's sophistication is evolving in post-case compliance enforcement. The Wyndham settlement is more audit-like than previous settlements. Most settlements call for an “assessment,” not an “audit.” Assessments are a statement by an outside expert on a series of claims made by managers. Audits, on the other hand, identify a standard and test the firm has met it.

The Wyndham settlement is notable because of the minimal amount of “fencing in” relief obtained by the Commission. For a variety of reasons, most respondents roll over when the FTC calls. Wyndham, perhaps because its franchise model was threatened by the FTC's action, was unwilling to roll. Wyndham was vigorously represented, and the case is a salient example of a respondent that kept the agency limited to addressing the articulated injury, rather than the broader problem of insecurity. Wyndham could be the first of many battles where respondents fight back, particularly to resist fencing in.

The lack of fencing in is unfortunate because we are learning that non-card breaches are often highly privacy invasive. For instance, mere disclosure of one's membership on Ashley Madison (the dating website for married people) is probably more harmful than having a credit card number stolen. The Sony breach and others are beginning to establish that exposure of ordinary business records can be as harmful as credit card numbers.

BLOOMBERG BNA: Does the Payment Card Industry Data Security Standard assessment to demonstrate compliance in essence provide Wyndham a safe harbor?

The approach is different and is a mixed bag for the Commission. On one hand, the changes demonstrate that the Commission's sophistication is evolving in post-case compliance enforcement. The Wyndham settlement is more audit-like than previous settlements. Most settlements call for an “assessment,” not an “audit.” Assessments are a statement by an outside expert on a series of claims made by managers. Audits, on the other hand, identify a standard and test the firm has met it.

The FTC's order makes it clear that Wyndham loses the benefits of having a clean assessment if it makes misrepresentations or if it makes material changes to its technical setup. These are meaningful, easy to violate exceptions. Because there is no mens rea attached to a misrepresentation, presumably any misrepresentation, including one made accidently, would suffice. Also, companies do change their architecture in order to game assessments. We see in PCI-DSS over and over again that companies are certified as PCI-DSS compliant, but then a breach happens and a post-breach analysis shows non-compliance.

The presumption of data security compliance if Wyndham obtains a clean PCI-DSS assessment is important because it is in effect a safe harbor from civil penalty/contempt actions. The FTC will have to go to court and overcome that presumption.

On the other hand, the PCI approach is a snapshot in time of compliance. The assessments, for all their warts, concern the operation of privacy and security programs over a long period of time. Thus, PCI is a more definite and objective standard, but it only deals with the narrow issue of card security, and only at one moment in time.

I think the next case to pay attention to is LifeLock, especially for those concerned that FTC actions do not afford adequate due process. Unfortunately, the case is sealed. But publicly-available information suggests that the case deals with information security. LifeLock publicly responded to the case by stating that it hired high-quality assessors to evaluate the company, that LifeLock spent millions to ensure compliance with the order, and that “[e]very audit completed by those third parties affirmed that we were in compliance.” Nonetheless, LifeLock has set aside over $100M to settle the case. Those who say they are concerned about FTC due process should try to get this case unsealed in order to understand how a company can have a clean assessment and yet receive a precedent-setting fine.

BLOOMBERG BNA: Is there anything to be gleaned from the fact that this was a no fault agreement?

Former FTC Commissioner Thomas Rosch has argued the broad denials of facts in settlements stretch the limit of what matters can meet the FTC’s “public interest requirement.” The Commission responded to this critique by promising it would strongly disfavor such denials, but broad denials continue to surface in consent agreements. Presumably, respondents want them to avoid subsequent action by attorneys general and class attorneys.