

## Privacy MVP: Ropes & Gray's Doug Meal

By Allison Grande

*Law360, New York (December 9, 2016, 6:16 PM EST)* -- Only Wyndham and LabMD have chosen to fight rather than immediately settle inadequate data security claims lodged by the Federal Trade Commission, and both have turned for assistance to Doug Meal, a Ropes & Gray LLP partner with a reputation for helping Target, Supervalu and a slew of others navigate the aftermath of high-profile data breaches, earning him a spot among Law360's 2016 Privacy MVPs.

Meal, who is being recognized as a Privacy MVP for the fifth year in a row, and the fellow members of the privacy and data security group he co-chairs have had a hand in the response to nearly every major data breach that has occurred in recent years, assisting companies ranging from Target and Home Depot to Supervalu and Neiman Marcus in navigating class action litigation, regulatory probes and other fallout that typically follows massive consumer data thefts.

Meal continued to build on his already impressive resume during the past year by not only securing favorable outcomes for his existing clients, but also by attracting a new client for which his firm has already scored a promising result.

"The success I've been able to have doesn't have anything to do with me," Meal told Law360. "We have an extremely strong team here from top to bottom, both on the enforcement side and compliance side, and because of that brand, we have been fortunate enough to get clients to allow us to handle high-profile matters for them and have been good enough to get good results for the clients that hire us. There's no secret sauce; it's not about marketing or having a cool, glossy website. It's about doing a great job for every single client. That's what gets you hired for the next one."

The Boston-based privacy pro kicked off his year by wrapping up longstanding work for Wyndham, which in 2012 became the first company to push back at a data security challenge mounted by the FTC. Specifically, the regulator alleged that the hotel chain violated the unfairness and deception prongs of Section 5 of the FTC Act by failing to maintain reasonable and appropriate security measures that could have prevented at least three breaches that occurred at Wyndham-branded hotels between 2008 and 2010.



After the Third Circuit affirmed in August 2015 that the FTC has the authority under the unfairness prong of Section 5 to regulate private companies' data security practices, the parties announced in December that they had reached a settlement. But while the dispute ended the same way that all but one of the commission's more than 50 other data security enforcement actions to date have, Meal noted that the terms of the resolution varied greatly from the deals that the regulator usually strikes with companies.

"I would put the things about the settlement into two buckets: the things that were in the settlement, and the things that weren't in the settlement, which in some ways ended up being more significant than what was in the order," Meal said.

He explained that, unlike in the scores of other consent decrees that have come out of FTC enforcement actions, the resolution in the Wyndham case applies to only payment card data and not to personal information more broadly. The pact also contained a provision that allows the hotel chain to be deemed in compliance with the comprehensive information security program that it is required to maintain under the agreement if it successfully obtains an annual audit that finds it to be in compliance with the Payment Card Industry's Data Security Standard, and the deal additionally refrained from holding the hotel chain responsible for its franchisees' data security practices.

"The bottom line is that the settlement wound up being a much better resolution for Wyndham than would have been available under a typical FTC consent decree," Meal said, adding that Wyndham felt "quite vindicated" in its decision to litigate.

Meal, who received his J.D. from Harvard Law School and his B.A. from the University of Pennsylvania, began his career as a general business commercial litigator and, like many in the privacy field, fell by chance into the practice area in which he has excelled after receiving a phone call one day nearly a decade ago from longtime client TJX Cos. Inc., the parent company of T.J. Maxx and Marshalls.

"I actually have the date marked on my calendar, Dec. 18, 2006, when I got that call from T.J. Maxx about a data breach that they had suffered," Meal recalled. "The day that I got that call, I'd never heard of privacy or data security law. I actually wondered why they were calling me and said to them, 'Shouldn't you be calling the police?'"

That day, which Meal plans to commemorate later this month, led to "quite a turn" in his career, with his work for T.J. Maxx on the various regulatory and legal entanglements prompted by the breach snowballing into the robust privacy and data security practice that Meal and his firm have built up today.

"Frankly, back in 2006, people like me didn't exist; there wasn't a go-to person or go-to people for data breach situations," Meal said. "That's what makes this area of law so unique and interesting and challenging, that the law is just extraordinarily undeveloped and nearly every decision is one of first impression that gives practitioners and other courts guidance in terms of how to resolve the cases and legal issues that come before them."

--Editing by Jack Karp.