Published on *The National Law Review* https://natlawreview.com

Two Regulatory Crises: Cybersecurity Issues

Article By:

David Smyth

It strikes me that two civil regulators are facing dire attacks on aspects of their enforcement programs – both in different ***U.S. Courts of Appeals*** – at the same time. Both of these attacks arise out of generalized statutes that only sort of address the problems the regulators seek to remedy. To some degree, how these matters are resolved will determine whether these enforcement portfolios are reinvigorated or whither on the vine. In both cases a Congressional fix could be in order.

The SEC's Insider Trading Enforcement Program

The ***Securities and Exchange Commission*** has had a mess on its hand since ***United States v. Newman***, a criminal case in the Second Circuit, was handed down last November. The core holding was this: to be liable for insider trading in a tipper/tippee context, (1) a tippee must know about the personal benefit received by the tipper for the information, and (2) while the personal benefit need not be immediately pecuniary, it must be "of some consequence" and mere friendship is not enough to qualify.

The case is important because many of the SEC's and Justice Department's insider trading matters fall into this tipper/tippee category. And a significant number of those are "remote tippee" cases, where a tipper gives material, nonpublic information to one tippee in exchange for a personal benefit of some kind, who then passes it to another who trades on it. In those matters, it can sometimes be hard to establish that the third-level (or fourth level or whatever) tippee knew about the personal benefit received by the tipper for the information. Also, to this point the personal benefit element has been quite lax, and has in many instances amounted to nothing more than the "warm glow" that comes from helping a friend. Applying more rigor in this area could put a real dent in law enforcement's efforts to police insider trading.

Recently the Second Circuit declined to rehear *Newman* en banc, and the U.S. Attorney's Office has not decided whether to pursue an appeal to the U.S. Supreme Court. Judge Rakoff, who is not exactly afraid of defying Congress and higher courts, recently denied a motion to dismiss in *SEC v. Payton*, an insider trading case where the defendants invoked *Newman*. Some have suggested that because Rakoff cited the SEC's lower burden of proof – recklessness as opposed to willfulness that the Justice Department must meet – the SEC could avoid many of the problems associated with *Newman*'s rationale.

I'm not so sure. *Payton* was a case decided on the pleadings, and Judge Rakoff held that the SEC's complaint was sufficient to survive a motion to dismiss. And it may have a generally easier time proving a tippee's knowledge of the personal benefit with its lower standard of proof. But it's still going to have to prove those facts. In *Newman* itself, the court held that prosecutors hadn't offered *any* evidence that the remote tippees knew what the personal benefit to the original tipper was. With that kind of showing, it won't matter what the burden of proof is. I'm also not sure the nature of the personal benefit will be dramatically affected by the burden of proof. If *Newman* is in effect, the personal benefit will either be "of some consequence" or it won't. I don't see that call being swayed depending on whether it's a criminal or civil case.

All of this uncertainty fundamentally derives from the generality in the statute typically used to prohibit insider trading – Section 10(b) of the Exchange Act. As we've discussed, it doesn't mention insider trading, just securities fraud, and that lack of specificity creates lots of opportunities for doctrinal confusion. Anyway, a number of proposals to define insider trading once and for all are in the works. We'll see if one of them gets through and makes *Newman* a moot point.

The FTC's Cybersecurity Enforcement Program

Meanwhile, the Federal Trade Commission has a similar issue with its cybersecurity enforcement program. Here's how the FTC defines its authority in this area:

> When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up [to] these promises. As of May 1, 2011, the FTC has brought 32 legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information. In these cases, the FTC can charge the defendants with violating of Section 5 of the FTC Act, which bars "unfair and deceptive acts and practices in or affecting commerce."

Um, okay! It's not crazy to think that some misconduct in the cybersecurity area would be unfair or deceptive, but Section 5 is a pretty broad statute for the FTC to rely on in all instances. What if, say, a company implements measures to protect itself against an electronic data breach and suffers a breach anyway? If the FTC thinks those measures were unreasonable were they also unfair or deceptive? Is the FTC authorized to use Section 5 to bring a case alleging as much?

That question is currently pending before the Third Circuit in a case that began back in 2012, when the FTC sued Wyndham Worldwide Corp. for alleged data security failures that enabled three data breaches between 2008 and 2009. The FTC charged Wyndham with violating both the deception and unfairness provisions of Section 5. Wyndham moved to dismiss in the U.S. District Court in New Jersey, challenging the FTC's authority to regulate data security. The court denied the motion, and Wyndham petitioned for an interlocutory appeal, which the Third Circuit granted last August.

The Court of Appeals asked counsel two questions in advance of oral argument, and then asked for supplemental briefing on these questions after oral argument :

- Has the FTC declared that unreasonable cybersecurity practices are "unfair," 15 U.S.C. § 45(a), through the procedures in the Federal Trade Commission Act, 15 U.S.C. §§ 41-58?

- Assuming it has not, is the FTC asking the federal courts to determine that unreasonable cybersecurity practices are “unfair” in the first instance, and if so, can the courts do so in this case brought under 15 U.S.C. § 53(b)?

All of this would likely be unnecessary with a more specific statutory and regulatory scheme in place. Counsel for the FTC said at oral argument that rulemaking in the cybersecurity area is “a very cumbersome process,” and that “it would never end because the technology changes so fast.” Perhaps needless to say, Wyndham disagrees. It argues that the FTC has previously used the rulemaking procedures to clarify unfairness in other contexts, and also points to several statutes – including COPPA, the FCRA, and Gramm-Leach-Bliley – that require the FTC to promulgate cybersecurity rules.

I can’t help but think that if the FTC loses this battle a new statute will be forthcoming from Congress. We’ll see what happens soon enough.

National Law Review, Volume V, Number 111