AntitrustConnect Blog

The FTC: a Tough Data Security Cop

David Balto (Law Offices of David A. Balto) · Monday, November 18th, 2013

Protecting data security is the most important consumer protection issue for the economy. Each year the Federal Trade Commission receives a flood of identity fraud complaints. Efforts to diminish the problem by noting the limits on consumer liability are just plain wrong. There are liability protections but the external costs can be overwhelming. Consumers must pay for credit repair services or insurance against credit fraud which cost over $7.5 billion annually. Consumers also have to spend a substantial amount of time resolving identity theft (estimated at 21 hours in a 2009 study). The harm does not end there. Identity theft can lead to debt collection harassment, lost employment opportunities, higher interest rates, lower credit availability, and higher insurance premiums. The emotional distress cannot be measured.

Luckily, we have a tough data security cop—the Federal Trade Commission—which has brought over 30 consumer privacy cases as of May 1, 2011.

Almost 100 years ago Congress created the FTC with broad powers to police, educate and regulate. Today, the FTC is the leading consumer protection agency and is modeled around the world. The FTC was vested with flexible powers to meet the evolving challenges facing our economy through Section 5 of the FTC Act, which bars unfair and deceptive acts and practices. In the past few years the FTC has used Section 5, in combination with other laws, to confront the tremendous need to protect consumer data.

But now those who oppose sensible enforcement have criticized the FTC for going too far. They suggest that the FTC is over-enforcing by challenging a lack of proper data security practices as unfair. This battle is being played out in a case involving Wyndham Hotels.

In *FTC v. Wyndham*, the facts are simple. Wyndham had lax security measures that led to three different security breaches over two years which allowed hackers to make off with over 600,000 payment card accounts which were exported to a domain registered in Russia. These accounts were used to make fraudulent purchases using the customer accounts. Wyndham's website states that they "safeguard our Customers' personally identifiable information by using industry standard practices." The statement goes on to say that Wyndham uses encryption to protect credit card numbers and financial data transmitted through their websites. But neither of these promises was kept.

Unfortunately, those who want less regulation not more wish to shackle the FTC's ability to use its power to challenge unfair data security practices. The Chamber of Commerce submitted an *amicus* brief calling Wyndham the victim and accusing the FTC of terrorizing the company. They accuse

the FTC of overreaching their Section 5 authority by claiming Wyndham's actions were unfair. The Chamber of Commerce could not be more wrong.

Section 5 allows the FTC to attack unfair conduct. An unfairness claim requires (1) substantial injury to consumers, (2) injury that was not reasonably avoidable by consumers, and (3) that the injury was not outweighed by countervailing benefits to consumers or competition. Each of these elements is clearly met in this case. Storing sensitive payment card information in readable text was below any industry norm and clearly wrongful conduct. Wyndham caused substantial injury to consumers that could have been prevented by readily available and low cost measures. The injury was not reasonably avoidable because consumers relied on false promises of data security. The true victims here were consumers, not Wyndham. Wyndham was like a person entrusted to store other people's valuables, then left those valuables in an unlocked car parked in a neighborhood known for theft.

The unfairness provision of Section 5 is a vital tool in protecting consumers from companies with substandard data security. To date the FTC has mainly relied on its deception authority – prosecuting companies that have violated their privacy promises – to punish clear deceptive conduct among companies that leave consumer data open to theft. But it is time for the FTC to fully utilize its unfairness authority to attack cases of inadequate data protection. An unfairness claim is particularly necessary, since consumers cannot engage in self-help—consumers cannot feasibly conduct their own examinations of companies' data security measures before giving them their valuable data.

In evaluating this debate we need to remember the extremely limited tools to prosecute data security violations. Consumers have extremely limited tools to sue to secure redress when companies fail to protect their data. The state attorneys generals have limited tools. The FTC stands nearly alone to protect our data.

In *Wyndham* and other cases, the FTC is going after practices that are grossly at odds with responsible industry standards. However, deception actions should not be the only enforcement tool. FTC enforcement is critical and they should not be shackled by having one hand tied behind their back. Consumers need a tough privacy cop.

This item originally appeared in The Huffington Post.