Montgomery & Hansen LLP

Client Alert September 1, 2015

Court Affirms FTC's Authority to Sue Companies for Inadequate Cybersecurity Protection

By **Daniel Appelman**

Last week the United States Court of Appeals for the Third Circuit unanimously affirmed the Federal Trade Commission's authority to bring legal action against companies that fail to employ reasonable cybersecurity measures to protect non-public consumer data.[1]

Section 5 of the Federal Trade Commission Act (the "FTC Act") gives the FTC authority to seek legal remedies against those who engage in "unfair or deceptive acts or practices affecting commerce."[2] The FTC has brought dozens of enforcement actions against companies alleging that their inadequate cybersecurity practices constitute unfair practices under Section 5. Until this decision, however, it was not clear whether the FTC actually had the authority under Section 5 of the FTC Act to regulate inadequate cybersecurity practices as unfair acts or practices. The Third Circuit answered this question in the affirmative.

Background of the Case

On three occasions in 2008 and 2009, hackers broke into the computer systems of Wyndham Worldwide Corporation and stole personal and financial information belonging to hundreds of thousands of its customers. In 2012, the FTC sued Wyndham and its subsidiaries in federal district court for engaging in unfair practices by failing to provide reasonable security measures to protect consumer data collected through its property management system and computer network, and for having a deceptive privacy policy. Among other things, the FTC alleged that the hackers had obtained payment card information from over 619,000 customers resulting in at least $10.6 million in fraud losses, and that Wyndham had failed to improve its cybersecurity practices even after it had experienced the second breach. Wyndham filed a motion to dismiss the lawsuit on the basis that the FTC lacked authority to regulate cybersecurity practices. The District Court denied Wyndham's motion to dismiss, and Wyndham appealed. The Third Circuit affirmed the District Court's decision to deny dismissal of the case, holding that the FTC does have authority to regulate cybersecurity practices and seek remedies from those whose cybersecurity practices are inadequate.

Liability Under FTC's Enforcement of Cybersecurity Practices

The potential liability for engaging in unfair or deceptive practices under the FTC Act is substantial. The FTC can seek three types of remedies in court: (i) civil penalties of up to $16,000 per violation of an FTC regulation; (ii) recovery of losses suffered by consumers; and (iii) injunctive relief that enables the FTC to freeze assets, rescind contracts and impose temporary receivers on violators. More often, companies charged with violations settle with the FTC by agreeing to implement better security measures and agreeing to be subject to outside monitoring.[3]

Key Lessons From This Decision

Lax Cybersecurity Measures May Constitute "Unfair Practices" Under Federal Law. The Third Circuit's decision confirmed that lax cybersecurity measures may constitute unfair practices under the FTC Act and that the FTC has the authority to sue violators. Although the decision is procedural and not determinative of Wyndham's liability on the merits, and although it is only precedential in the Third Circuit, it has broad significance for all companies that collect and retain personal information about consumers.

FTC's Enforcement Actions Do Not Require Advance Notice of What Measures Constitute Reasonable and Unreasonable Cybersecurity Practices. Wyndham had argued that the FTC's failure to provide it with notice as to the

For more information about cybersecurity protection, please contact Daniel Appelman at dappelman@mh-llp.com or at 650-331-7014.

specific security measures it considered reasonable and unreasonable made the FTC's enforcement action unconstitutional as a violation of due process. The court rejected that argument and, perhaps significantly for future cases, appears to have agreed with the FTC that preexisting industry guidelines, a published FTC guidebook and the complaints filed in previous FTC enforcement actions serve to give companies ample notice as to what constitutes reasonable security programs.[4]

FTC's Allegations Against Wyndham Puts Other Companies on Notice. The FTC's allegations of wrongdoing against Wyndham serve as a warning to every company that collects personal information from consumers. Those allegations included: (i) allowing the use of easily guessed passwords, (ii) failing to use readily available security measures, such as firewalls and encryption, (iii) failing to employ reasonable measures to detect and prevent unauthorized access, (iv) failure to follow proper incident response procedures, and (v) failure to monitor its network for malware used in the previous intrusions into Wyndham's systems. The FTC expects companies collecting private consumer data to take reasonable measures to safeguard that data and avoid committing the same mistakes as those made by Wyndham.

Implications for Privacy Policies. In addition to its authority to regulate unfair practices, Section 5 of the FTC Act also gives the FTC authority to take action against *deceptive* acts. In the original complaint against Wyndham in Federal District Court, the FTC alleged that Wyndham engaged in deceptive acts by misrepresenting its actual cybersecurity practices in its privacy policy. For example, Wyndham's privacy policy claimed that it used "industry standard" security measures to protect consumer data as well as firewalls and 128 bit encryption, but in fact it did not, according to the FTC. Although the Third Circuit didn't squarely address this issue (because Wyndham failed to raise it on appeal) it did refer disapprovingly to Wyndham's false representations;[5] and those representations may be an additional basis for the District Court to assess Wyndham's liability if the case proceeds to a trial. The take-away here is that companies should periodically review their privacy policies to confirm they accurately reflect their actual cybersecurity practices.

Conclusion

Given the significant security breaches reported from Target, Sony, JP Morgan Chase, Home Depot, Neiman Marcus, Anthem and others, federal and state governments are becoming increasingly aware of the need to enact strong data protection laws and to give their law enforcement and regulatory agencies broad authority to police lax cybersecurity practices. The Wyndham case makes clear that the FTC expects companies collecting private consumer data to employ reasonable cybersecurity policies, programs and procedures that adhere to industry standards and take notice of the guidance provided by the FTC in public statements and its previous consent decrees.[6] These policies, programs and procedures must be regularly reviewed and updated to account for changes over time in technology, company practices and legal and regulatory requirements.

Practice Tips

In view of the highlighted authority of the FTC to regulate in this area, clients collecting personal information from consumers can minimize the risk of an enforcement action by doing the following:

- Assume that your company will be a target for hackers and plan accordingly. Don't wait to institute good security measures until after you are attacked.
- Deploy regularly updated firewalls, antivirus, and web security solutions throughout
- your network.
- Change passwords frequently, especially administrator passwords; and don't allow easily guessed passwords.
- Map your consumer private data so you know where it is, where it is moved, where it is backed up and archived, and what protections are in place to secure it.
- Use strong encryption for protecting sensitive data, particularly personal and financial information belonging to consumers.
- Limit access to only those employees who have a "need to know"; and require them to change their passwords frequently. Each such employee should have his/her own user account with a unique user name and password to enhance accountability and traceability.
- Back up sensitive data frequently.
- Update software frequently—intruders often find and use flaws in operating systems and browsers that are subsequently fixed by the vendors in updates.
- Limit administrator privileges to prevent installation of unauthorized software.
- Perform background checks on employees having any access to sensitive information or data.

- Develop an incident response plan with written procedures; and designate an appropriate incident response team.
- Document breaches systematically and in writing when they occur.
- Keep abreast of changing industry and FTC guidelines, including the guidance provided by previous FTC enforcement actions.
- Determine whether outside help is needed to terminate the breach, prevent recurrence and comply with notification and other legal requirements.

[1] Federal Trade Commission v. Wyndham Worldwide Corporation (No. 14-3514)

[2] 15 U.S.C. § 45(a).

[3] The FTC is not the only governmental entity charged with enforcing cybersecurity practices to protect consumer data. For example, California's Information Practices Act, which is part of the California Civil Code, now requires businesses that own, license or maintain personal information about California residents (including consumer information) to implement and maintain reasonable security procedures and practices to protect that personal information from unauthorized access, destruction, use, modification or disclosure. Cal. Bus. & Prof. Code §§ 17200, 17202-17206. Violations of that law can be enforced through the remedies provided by California's Unfair Competition Law. Other states have similar laws.

[4] FTC v. Wyndham at 41.

[5] FTC v. Wyndham at 17.

[6] Both the FTC and the California Attorney General have issued guidelines for cybersecurity "best practices". FTC guidelines. California guidelines.