TOP 10 CYBERSECURITY TIPS FOR BUSINESSES

FOLLOWING FTC V. WYNDHAM

By Matthew Nelson, Corporate Strategy Attorney, Symantec

The Federal Trade Commission (FTC) has long been recognized as America's consumer watchdog, but some have bristled at the increasing role the FTC plays in regulating the cybersecurity practices of global businesses. Since 2002, the FTC has relied on Section 5 of the FTC Act (codified as 15 U.S.C. § 45(a)) to secure more than 50 settlements against businesses for allegedly deficient cybersecurity practices that failed to protect consumer data against hackers. Section 5 prohibits businesses from engaging in "*unfair or deceptive* acts or practices in or affecting commerce" (emphasis added).

Although the FTC's authority to regulate businesses outside the banking, telecommunications and transportation sectors has existed since 1914, the scope of the FTC's authority to regulate cybersecurity practices under the "unfairness" prong of Section 5 has remained unclear. Most of the FTC's early consumer privacy cases hinged on their statutory authority under the "deception" prong of Section 5. The cases typically targeted companies for providing false data security or privacy representations to consumers via their company websites and applications. However, the cases settled since the deceptive nature of the policies was often obvious and businesses preferred to avoid negative publicity than fight.

Contrary to these routine "deception" cases, the FTC's authority to regulate the cybersecurity practices of businesses under Section 5's "unfairness" prong has been less clear. The FTC first asserted "unfair" cybersecurity practices in 2005,[1] and like the "deception" cases, the "unfairness" cases settled. Common settlement terms required defendants to train employees, implement data security safeguards and undergo independent security assessments biannually for twenty years.

Although some defendants questioned the FTC's authority to regulate the cybersecurity practices of businesses under the "unfairness prong" so broadly, they capitulated to the FTC's demands rather than engage in a prolonged and potentially embarrassing public legal battle. All that changed in 2012 when the FTC filed a complaint against Wyndham Worldwide Corporation (Wyndham) alleging Wyndham engaged in "unfair" cybersecurity practices

that unreasonably exposed consumers' personal data to unauthorized access and theft.

The FTC's Allegations and Wyndham's Response

In *Federal Trade Commission v. Wyndham Worldwide Corp.*, 799 F.3d 236, (3d Cir. 2015) the FTC alleged Wyndham's poor cybersecurity practices led to hackers stealing personal and financial information from hundreds of thousands of consumers on three different occasions between 2008 and 2009. They further alleged the theft resulted in fraudulent charges exceeding $10.6 million dollars. Rather than settle, Wyndham challenged the FTC's authority on numerous grounds, only two of which were certified on appeal. First, Wyndham challenged the FTC's cybersecurity policing authority under Section 5 of the FTC Act. Second, Wyndham argued that even if the FTC possessed Section 5 authority, they failed to provide "fair notice" of what was required of Wyndham and other businesses.

On August 24, 2015, the United States Court of Appeals for the Third Circuit helped solidify the FTC's Section 5 authority by unanimously rejecting both of Wyndham's arguments. Although the court hinted a different "fair notice" argument may have persuaded the court to rule differently,[2] Wyndham elected to settle with the FTC on December 9, 2015.

Among other things, the settlement requires Wyndham to establish a comprehensive information security program to protect cardholder data. The company must also conduct annual information security audits for 20 years and report any data breaches affecting more than 10,000 payment card numbers to the FTC within 10 days.The FTC's press release about the settlement contains additional details and a link to the stipulated agreement.[3]

In another interesting twist, an administrative law judge dismissed a similar case on different grounds a few months after Wyndham. In *In re LabMD Inc.*, Docket No. 9357, ALJ's Initial Decision (F.T.C. Nov. 13, 2015), Chief Administrative Law Judge Chappell dismissed the FTC's case after finding that the FTC's regulation of unfair practices requires a showing that consumer harm is "probable" not just "possible." Although the administrative decision in LabMD carries persuasive authority, it is not binding on federal and state courts and it has been appealed by the FTC. Additionally, even if the ruling survives appeal, LabMD and Wyndhamare distinguishable.

What does Wyndham Mean for Businesses?

The ramifications of the Wyndham decision are significant because the FTC's authority to regulate cybersecurity practices under the "unfairness" prong of Section 5 of the Act has finally been judicially validated by an appellate court. The decision is also important because it means the FTC's guidelines and enforcement activities essentially define the standard of cybersecurity care required by businesses that fall within the scope of the FTC's regulatory authority. Barring a contradictory appellate court ruling, the issuance of formal rules or guidance, or legislative action, the FTC's required standard of care for cybersecurity is likely to evolve as new guidelines are issued and new cases are decided.

Foreign businesses and U.S. businesses outside the scope of the FTC's regulatory authority are even impacted by Wyndham. The FTC has been the most active federal privacy regulator in the United States, has published the most privacy guidelines, brought the most privacy enforcement actions and worked with hundreds of privacy authorities and organizations around the world. The FTC is also responsible for enforcing the newly proposed EU-US Privacy Shield agreement addressing the transfer of personal data from Europe to the United States.. This combined influence makes the FTC's position on the standard of care necessary to protect consumer privacy extremely important both domestically and internationally

The standard of care most recently articulated by the FTC requires businesses to take "reasonable and necessary measures" to protect consumer data. Although the FTC has not provided bright line rules defining what constitutes "reasonable and necessary measures" for implementing a cybersecurity program, they have provided guidance.

For example, the FTC's website contains tips and advice for businesses[4] and published settlement agreements.[5] Commission leaders have also engaged in public outreach[6] in an effort to educate industries within their jurisdiction. Arguably, however, the most important of all these resources is the FTC's recent publication in June of 2015 titled: *Start with Security, A Guide for Business, Lessons Learned from FTC Cases*.[7] Considering the court in Wyndham relied on the publication of an earlier FTC guidebook in 2007[8] to support its position that Wyndham had notice of what was required, the importance of the new 2015 guide cannot be overemphasized.

The 2015 guide distills important facts from over 50 FTC cases into 10 important lessons that are summarized below. Heeding these lessons will help any business streamline implementation of "reasonable and necessary" cybersecurity measures to protect sensitive data. Perhaps more importantly, adhering to these standards may help businesses avoid or minimize enforcement scrutiny in the event a data breach or loss occurs.

1. Start with Security

Although securing sensitive information is critical, no one can steal what you don't possess. That means organization should limit the collection of consumer information to only what they need. Keeping information longer than necessary and for reasons other than legitimate legal or business purposes makes no sense. Eliminating stockpiles of useless information should be part of a good data security plan that feeds into your organization's broader information governance[9] strategy.

2. Control Access to Data Sensibly

If there is a legitimate legal or business purpose for holding sensitive data, reasonable steps should be taken to secure that data. That not only means protecting data from outsiders, but also limiting access to those requiring access. Training employees and segregating sensitive data can go a long way toward controlling access to data. However, the risk of loss and theft can be further reduced and streamlined with data loss prevention technology designed to automate data access rules and detect suspicious user behavior.

3. Require Secure Passwords and Authentication

Requiring employees and customers to use complex and different passwords is a critical data protection step that is commonly overlooked. Passwords like "admin" or "1234" are not much better than not using a password. Similarly, storing password credentials securely is necessary to prevent bad guys from accessing your password piggy bank. Pass phrases that include numbers and unique characters are stronger and far less likely to become compromised, while including the use of two factor authentication adds an even stronger layer of security.

4. Store Sensitive Personal Information Securely and Protect it During Transmission

Data doesn't stay in one place, but sensitive data should be secured at all times. If transmitting information is necessary for your business, the data should be encrypted and secured during the transmission using industry tested standards and reliable technology. Remember, technology is not enough. Make sure encryption technologies are properly configured, deployed and updated or they may be ineffective.

5. Segment Your Network and Try to Monitor Who is Trying to Get In and Out

Firewall tools are an important way to segregate your network and to prevent the spread of digital diseases like viruses and malware across the organization. Similarly, intrusion detection and prevention monitoring tools may be able to prevent unauthorized access or at least limit damage if the network is penetrated. Tools and services exist to help monitor for malicious activity. Failure to use them may be a red flag for the FTC.

6. Secure Remote Access to Your Network

If employees, clients or service providers are given remote access, steps should be taken to secure remote access to the network. Limiting what can be remotely accessed in your network and using firewalls is a logical first step. However, securing the computers and other devices used to remotely access the network with anti-malware software and other endpoint protection software is equally important.

7. Apply Sound Security Practices When Developing New Products

If you plan to ship the hottest new "app" or software product, have you thought about whether customers will use your solution to store or send personal data? If they will, then you need to make sure the data is secure. That

means training engineers to use secure coding practices that prevent or reduce the risk of introducing security flaws during product design. Following platform guidelines when writing code along with testing and verifying privacy features prior to deployment are important steps that can help reduce security risk.

8. Make Sure Your Service Providers Implement Reasonable Security Measures

Implementing reasonable security within your organization alone is not enough. Third party service providers and business partners should be required to sign written agreements to provide appropriate security. However, the FTC has also indicated written contracts might not be enough because security can't be "a take our word for it" approach. Additional steps should be taken to actually verify that service providers and business partners are complying with your company's reasonable security standards.

9. Put Procedures in Place to Keep Your Security Current and Address Vulnerabilities That May Arise

Securing software and networks is an ongoing process that requires continuous monitoring and remediation. At a minimum, that means third party software must be updated regularly to patch vulnerabilities. Similarly, companies developing their own commercially available software should also have a process in place for reporting and addressing security vulnerabilities. Simple steps like regularly updating security software and establishing a routine reporting and correction procedure are fundamental components of a reasonable security strategy.

10. Secure Paper, Physical Media, and Devices

Sensitive information can easily be exposed when not properly secured regardless of whether it exists in paper or electronic format. Important paperwork should be maintained in secure locations and deleted when it is no longer needed. Similarly, media such as laptops, hard drives, flash drives and mobile phones should be properly secured so information can be protected if those devices are lost are stolen. Wiping hard drives and devices that are no longer in use and shredding unneeded paper documents helps eliminate downstream security risks.

Conclusion

Although the privacy threats facing consumers have evolved significantly since the FTC was established over one hundred years ago, there is no doubt the FTC and other regulators across the world intend to regulate the cybersecurity practices of businesses in today's modern landscape. The Wyndham decision validates the FTC's authority to regulate businesses and puts companies on notice that FTC guidelines and cases help form the standard for defining what constitutes "reasonable and necessary" security practices when it comes to consumer privacy. Adhering to these top 10 cybersecurity tips will not only help keep your business and consumer data safe,, you will also be better positioned to defend against inquiries from the FTC and other regulators if a breach or data loss occurs.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity solutions and services that make the world a safer place by delivering unmatched visibility and insights to customers and partners by providing a comprehensive approach to security. Our leading technologies, Global Intelligence Network (GIN), and cyber threat experts are here to help you build custom security solutions—on premise, in the cloud, and everywhere data travels. To learn more go to **www.symantec.com** or connect with Symantec at: **go.symantec.com/socialmedia**.

[1] See In the Matter of BJ's Wholesales Club, Inc., No. 042-3160 (June 16, 2005) (BJ's settles with FTC based on charges that its failure to take appropriate security measures to protect consumer credit and debit card information resulted in an unfair practice).

[2] The appellate court indicated Wyndham may have had an opportunity to argue for the application of a stronger "fair notice" requirement later in the proceedings. However, given the significant increase in settlements, guidelines and public outreach campaigns by the FTC since 2008, future defendants will be hard pressed to persuade courts they lacked "fair notice."

[3] Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk, (https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment (last visited Feb. 9, 2016).

[4] Federal Trade Commission, Tips for Businesses, https://www.ftc.gov/tips-advice/business-center (last visited Nov. 2, 2015).

[5] Federal Trade Commission, Privacy and Security Cases, https://www.ftc.gov/taxonomy/term/245/type/case (last visited Nov. 2, 2015).

[6] FTC Commissioner, Julie Brill and Matthew Nelson, Solving the Cybersecurity Puzzle Webinar, Inside Counsel http://www.insidecounsel.com/webseminars/solving-the-cybersecurity-privacy-puzzle (Mar. 17, 2015).

[7] Federal Trade Commission, Start with Security: A Guide for Business, Lessons Learned from FTC Cases, (Jun. 2015) available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

[8] Federal Trade Commission, *Protecting Personal Information: A Guide for Businesses*, (2007) available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

[9] Natasha Ratliff, *Is Your Organization's Data Management Plan a Ticking Time Bomb of Risk?*, Jan. 2015, Forbes Symantec Brand Voice, available at http://www.forbes.com/sites/symantec/2015/01/20/is-your-organizations-data-management-plan-a-ticking-time-bomb-of-risk/