
Federal Trade Commission Issues “Start with Security” Guidance

WEDNESDAY, JULY 01, 2015

On June 30, the Federal Trade Commission (FTC) issued its first guidance document as part of its *Start with Security* initiative. The initiative, announced by FTC Consumer Protection Director Jessica Rich in March, will initially focus on encouraging small and medium-sized businesses to embrace security-by-design principles. The initiative will include a series of FTC-hosted meetings across the country as part of the FTC’s education and outreach program. The first seminar, which will discuss guidelines for data security, will be held on September 9, 2015 at the University of California Hastings College of Law in San Francisco.¹

In the new guidance document, *Start with Security: A Guide for Business*,² the FTC draws what it considers to be lessons learned from 54 data security enforcement actions the Commission has brought since 2001. Based on a review of these cases, the FTC advises companies to incorporate a series of ten lessons learned:

1. **Start with security.** The FTC expects companies to develop an appropriate, proactive cybersecurity plan for the organization. Such a plan should address whether and when to collect sensitive, personal information and determine how long such information should be retained. Personal information should be collected and retained only as needed.
2. **Control access to data sensibly.** Companies should ensure appropriate access controls exist for both outward-facing and inward-facing systems.
3. **Require secure passwords and authentication.** When a company stores sensitive information on its network, the FTC expects the company to implement strong authentication requirements, including periodic password changes and limiting unsuccessful login attempts. Allowing employees or customers to use insufficiently complex passwords may be inadequate. Companies should store passwords securely.
4. **Store sensitive personal information securely and protect it during transmission.** The FTC expects organizations to use strong cryptography to secure sensitive personal information, both in transit and at rest. Companies should use industry-standard practices

and ensure that the measures in place are properly configured.

5. **Segment networks and monitor who's trying to get in and out.** The FTC expects companies to design their networks using tools like firewalls to ensure sensitive information is compartmentalized, and to install intrusion detection and prevention tools.
6. **Secure remote access to networks.** This includes ensuring endpoint security for computers with remote access to a company's networks, and restricting the scope of remote access only to what's necessary to get the job done. For example, third-party remote access to a network can be secured by restricting connections to specified IP addresses or granting temporary, limited access.
7. **Apply sound security practices when developing new products.** The guidance describes previous FTC enforcement actions where the FTC alleged failures to (a) train employees in secure coding practices, (b) follow explicit platform guidelines about secure development practices, (c) test privacy or security features, and (d) adequately assess applications for well-known vulnerabilities.
8. **Make sure service providers implement reasonable security measures.** Companies should "keep a watchful eye" on service providers, especially those processing personal information or developing applications. This includes taking reasonable steps in selecting providers, including contractual security standards, and conducting oversight.³
9. **Put procedures in place to keep security current and address vulnerabilities that may arise.** This includes updating and patching third-party software, heeding credible security warnings and moving quickly to fix them, and ensuring there is a process for reporting and fixing vulnerabilities identified in a company's own software.
10. **Secure paper, physical media, and devices.** Companies should take steps to secure important paperwork, protect devices (such as point-of-sale devices) that process personal information, protect sensitive information when removed from the company's workspaces (such as encrypting digital media, tracking shipments, and not leaving files unattended), and disposing of sensitive paper or media in a secure manner.

Implications

While the guidance notes that the findings are based on FTC complaints, rather than court findings, and that the specifics of the resulting orders apply only to those companies involved in the settlements, it states that "learning about alleged lapses that led to law enforcement [actions] can help your company improve its practices. And most of these alleged practices involve basic, fundamental security missteps." The guidance thus seems designed in part to respond to the criticism that, in relying on its authority to police "unfair" trade practices under Section 5 of the FTC Act, the Commission has failed to provide adequate notice of the standards by which it judges data

security practices.

Whether the FTC has authority under its Section 5 “unfairness” authority to bring data security claims is being challenged in the *Wyndham* litigation—where a decision from the Third Circuit is expected by the end of the year⁴—and in the *LabMD* case.⁵ The FTC has appeared to equate unfairness with falling below some standard of commercial reasonableness. Even if data security falls within the scope of the FTC’s “unfairness” authority, questions will remain about how and on what basis the FTC determines what data security practices are commercially reasonable for different kinds of businesses.⁶

This guide is the closest the FTC has come to providing a consolidated list of specific data security expectations, since it published *Protecting Personal Information: A Guide for Business* in 2011,⁷ albeit not one supported by evidence about how widespread these practices are in various economic sectors. Nonetheless, because the guidance reflects the FTC’s judgments about data security best practices, companies, particularly those storing or processing consumers’ personal information, may wish to carefully review their data security practices in light of this guidance.

¹ For more information on the FTC’s *Start with Security* initiative, see Federal Trade Commission Signals Intensified Focus on Security-By-Design and the Internet of Things With New *Start with Security* Initiative for Small and Medium-Sized Businesses, available at <https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=17179877274>.

² Federal Trade Commission, *Start with Security: A Guide for Business* (June 2015), available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

³ For more information on the FTC’s prior enforcement actions regarding vendor security issues, see D. Reed Freeman Jr. and Maury Riggan, *A Primer on FTC Expectations for Your Partner and Vendor Relationships: Enforcement Shows You Are Your Brother’s Keeper*, 14 PVLR 781 (May 4, 2015), available at https://www.wilmerhale.com/-/media/files/Shared_Content/Editorial/Publications/Documents/a-primer-on-ftc-expectations-for-your-partner-and-vendor-relationships.pdf.

⁴ *Federal Trade Commission v. Wyndham Worldwide Corp.*, No. 14-3514 (3rd Cir.) (argued Mar. 3, 2015).

⁵ *LabMD, Inc. v. Federal Trade Commission*, 776 F.3d 1275 (11th Cir. 2015).

⁶ Brief for Appellant at 35 et seq., *Federal Trade Commission v. Wyndham Worldwide Corp.*, No. 14-3514 (3rd Cir., Oct. 6, 2014) (“In particular, the FTC has provided no guidance on what cybersecurity practices business must adopt (or avoid) to comply with the law.”) The FTC rejected this argument, adopting the district court’s response, that Wyndham had adequate notice from FTC guidance documents and prior enforcement cases (which “are akin to policy statements or interpretive rulings, which, though not binding, reflect a body of experience and informed judgment to which courts and litigants may properly resort for guidance.” Supplemental Memorandum of the Appellee

at 3, *Federal Trade Commission v. Wyndham Worldwide Corp.*, No. 14-3514 (3rd Cir., March 27, 2015)).

⁷ Available at https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

Authors



**Benjamin A.
Powell**

PARTNER

Co-Chair, Cybersecurity and
Privacy Practice

Co-Chair, Artificial Intelligence
Practice

✉ benjamin.powell@wilmerhale.com

☎ +1 202 663 6770