Cooley

July 2, 2015

The Federal Trade Commission (FTC) has brought over 50 cases against companies that put consumer data at unreasonable risk. On June 30, 2015, the FTC released a guide titled *Start with Security* that summarizes 10 lessons the FTC has culled over the course of these cases.

These lessons can help your business protect consumer data, confidential data, and other proprietary information (together "sensitive information"). These lessons can also help you avoid FTC investigation. Data breaches and other consumer information issues are serious public relations problems, and the FTC has enforcement authority that includes the ability to obtain civil penalties for violations of FTC orders.

This alert first explains the general principles underlying the lessons. Then, it lists the 10 lessons, explains them, and points you to additional resources the FTC has made available. Finally, it provides information about ways to follow up if you still have questions or concerns.

The two major themes of the 10 lessons

The major themes of the lessons are twofold. First, data collection, use, and access should be limited as much as possible, while still allowing your business to operate. Second, your systems are only as secure as their weakest link. Both themes apply across a variety of contexts.

For example, applying the first theme, your organization should only collect, store, and use as much data as is necessary. Individuals within your organization should only have access to the data they need to do their jobs. Computers should only be as connected as they need to be to serve their function. And remote access should be only as extensive as it needs to be to allow your organization to operate.

Applying the second theme, all phases of data's lifecycle, from collection through use, transmission, and destruction, must be secure. Password protected systems are only as secure as the passwords that protect them. Devices that store information must be secure while they are moving as well as when they are at rest. And even if your systems are secure, weaknesses in third-party systems could undermine your efforts.

With these themes in mind, we turn now to the lessons.

The 10 lessons

First, "[s]tart with security." This means data security should be integral to every decision you make that involves sensitive information. The key is minimization. Your organization should collect the minimum amount of sensitive information it needs to operate. Such information should be kept only as long as necessary, and should not be used when unnecessary. Finally, data should be destroyed when it is no longer needed.

Second, "[c]ontrol access to data sensibly." This means that, within your organization, data should only be accessible to people who need it to do their jobs, and only as long as they need it. It is particularly important to limit administrative access, which allows users to make system-wide changes to your systems. Administrative access should be sharply restricted to only the users who need it.

Third, "[r]equire secure passwords and authentication." This means passwords should be complex, unique, and difficult to break—ideally involving strings of letters, numbers, and symbols. And passwords should be stored securely—no plain-text files. Your systems should also restrict the number of login attempts users can make, to obstruct "brute-force" login attempts. Finally, you should be sure that password-protected systems and information can't be accessed by going around the login, for example with easily-manipulable URLs.

Fourth, "[s]tore sensitive personal information securely and protect it during transmission." This means that information should be protected throughout its entire lifecycle, from collection through transmission, use, and destruction. Protection should meet industry-tested standards, which should be properly implemented. Security

experts have already put considerable effort into developing strong standards. Using such standards is more likely to keep your sensitive information safe, and may save you the expense of developing an appropriate proprietary system.

Fifth, "[s]egment your network and monitor who is trying to get in and out." This means you should use tools like firewalls to limit access among computers in your networks. The principle for computers is the same for people and companies: each system should have access to only the information it needs to serve the function it needs to serve within your organization. And your systems should automatically monitor attempts at unauthorized access.

Sixth, "[s]ecure remote access to your network." This means that if you allow your employees, customers, or other parties to have remote access to your network, you need to first ensure that your network is secure for remote access, and then ensure that your remote users also have appropriate security measures in place. Otherwise, hackers may be able to access your systems through third-party systems. A similar principle applies here as in the other lessons: remote access should be limited to the access necessary to allow employees or other parties to serve their appropriate functions.

Seventh, "[a]pply sound security practices when developing new products." Your engineers should be trained in secure coding practices, and your products should follow platform guidelines that platform developers provide. After development, you should test your products to make sure that their privacy and security features work, and that they are not vulnerable to common types of attacks.

Eighth, "[m]ake sure your service providers implement reasonable security measures." Your service providers should be contractually bound in writing to implement reasonable security measures, and you should have a mechanism available to verify compliance. No matter how secure your systems are, third-party failures might still result in a consumer data breach.

Ninth, "[p]ut procedures in place to keep your security current and address vulnerabilities that may arise." This means you should keep all software on your systems up-to-date and patched, as appropriate. And if there are credible vulnerabilities that come to your attention, you have an obligation to address them. It may be good, for example, to have a dedicated e-mail address just to receive security notices about such credible vulnerabilities

Finally, "[s]ecure paper, physical media, and devices." If you have paper files, they should be stored securely, rather than left in the open or in unlocked boxes. Similarly, devices like point-of-sale terminals that collect, store, or transmit personal information should be protected. And it is just as important to protect devices that store sensitive information while they are being shipped as it is when they are at rest—information on laptops, thumb drives or other devices should be encrypted, and these devices should be shipped by traceable methods.

When information is no longer needed, it should be destroyed securely.

Other resources from the FTC

In addition to these 10 lessons, the FTC has published other guidance, including: *Protecting Personal Information: A Guide for Business*; an online tutorial and other publications. These resources are available at no cost on the FTC website.

If you still have questions

This FTC guide contains crucial insights the FTC has collected over the course of over 50 enforcement actions. Please contact our Privacy & Data Protection team if you have any questions about how to implement these strategies or any other strategies to help keep your business and your clients secure in a complex and fast-changing environment.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Scott Dailard San Diego	sdailard@cooley.com +1 858 550 6062
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090