

Hearing #9 on Competition and Consumer Protection in the 21st Century

Constitution Center
December 12, 2018



Welcome

We Will Be Starting Shortly



Welcome

Jared Ho

Federal Trade Commission

Division of Privacy and Identity Protection



Data Security Assessments

Panel Discussion:

Malcolm Harkins, Carolyn Holcomb, Troy Leach, Tom McAndrew, Wendy Nather, Garin Pace

Moderators:

Elisa Jillson, Jim Trilling



Hypo #1

Company A was a start-up 10 years ago, with an innovative rent-a-pet model. The company now has over 150 employees in 3 locations. The company had no security personnel *per se* at first and then hired a few IT jack-of-all-trades to handle aspects of security. The founder has now hired a CISO for the time.

How should the CISO assess the company's security at this point in time? How should the CISO stay on top of the company's security?



Hypo #2

Company B is a mature company with an internal audit department, a large security staff, and a CISO who reports to the board. It plans to obtain new cyber insurance.

How should the CISO, the board, and prospective cyber insurers assess the company's security?

What types of information will prospective insurers request from Company B to assess its data security risks?



Hypo #3

Company C is a mid-sized firm that has long struggled with patch management and third-party vendor relationships. It hires a new CISO who wants to understand the scope of the problems and of the company's security generally.

How should the CISO assess the security situation?

How are these persistent problems relevant to Company C's ability to obtain cyber insurance?



Hypo #4

Company D starts processing payment cards for the first time.

How should the company assess its risk on day 1 of payment processing and going forward?



Hypo #5

Company E hires a penetration tester and discovers some significant vulnerabilities in systems that hold customer information, including payment card data. However, the company is going through a difficult financial time.

How should the company proceed?



Hypo #6

Company AA is required by FTC consent order to obtain biennial assessments. The company believes that system X does not contain any consumer personal information covered by the order, so it negotiates with its assessor a scope of work that takes system X out of review.

Setting aside legal issues, what are the implications for the assessment process of this carve-out?



Hypo #7

Company BB has annual PCI DSS audits and biennial FTC assessments (required by consent order). The PCI DSS qualified security assessor (QSA) and the FTC assessor identify a number of ways in which the company's security has not been consistent with the PCI DSS or the consent order. The company takes corrective actions.

What findings should the QSA and the FTC assessor make?



Data Security Assessments

Panel Discussion:

Malcolm Harkins, Carolyn Holcomb, Troy Leach, Tom McAndrew, Wendy Nather, Garin Pace

Moderators:

Elisa Jillson, Jim Trilling



Break

11:05-11:15 am



Fireside Chat: Emerging Threats

Participants:

Joshua Corman

Commissioner Rebecca Kelly Slaughter



Lunch Break

11:45 am-1:00 pm



The U.S. Approach to Data Security

Panel Discussion:

Chris Calabrese, Janis Kestenbaum, Daniel Solove,
Lisa Sotto, David Thaw

Moderator: James Cooper



Break

2:30-2:45 pm



FTC Data Security Enforcement

Panel Discussion:

Woodrow Hartzog, Geoffrey Manne, William McGeeveran,
Lydia Parnes, Michelle Richardson

Moderators:

Jim Trilling, Laura Riposo VanDruff



Closing Remarks

Maneesha Mithal

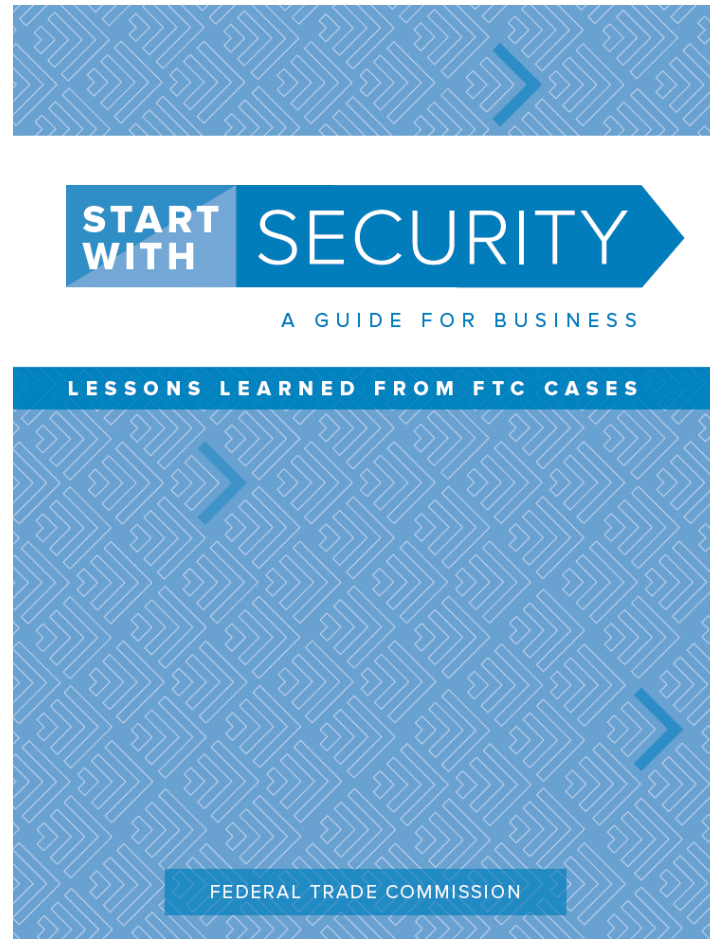
Federal Trade Commission

Division of Privacy and Identity Protection















Start with Security: Lessons Learned from FTC Cases

available at business.ftc.gov



Stick with Security: An FTC Business Blog series

available at business.ftc.gov

	Stick with Security: Insights into FTC investigations
	#1 Start with security – and stick with it
	#2 Stick with Security: Control access to data sensibly
	#3 Stick with Security: Require secure passwords and authentication
	#4 Stick with Security: Store sensitive personal information securely and protect it during transmission
	#5 Stick with Security: Segment your network and monitor who's trying to get in and out
	#6 Stick with Security: Secure remote access to your network
	#7 Stick with Security: Apply sound security practices when developing new products
	#8 Stick with Security: Make sure your service providers implement reasonable security measures
	#9 Stick with Security: Put procedures in place to keep your security current and address vulnerabilities that may arise
	#10 Stick with Security: Secure paper, physical media, and devices
	Stick with Security: FTC resources for your business



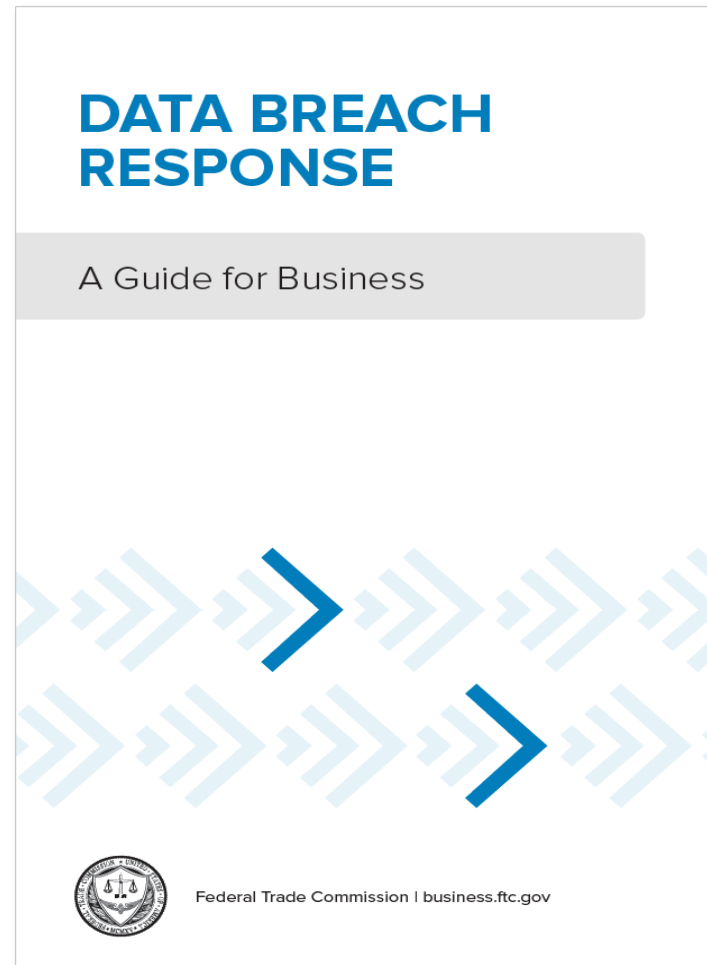
Careful Connections: Building Security in the Internet of Things

available at business.ftc.gov



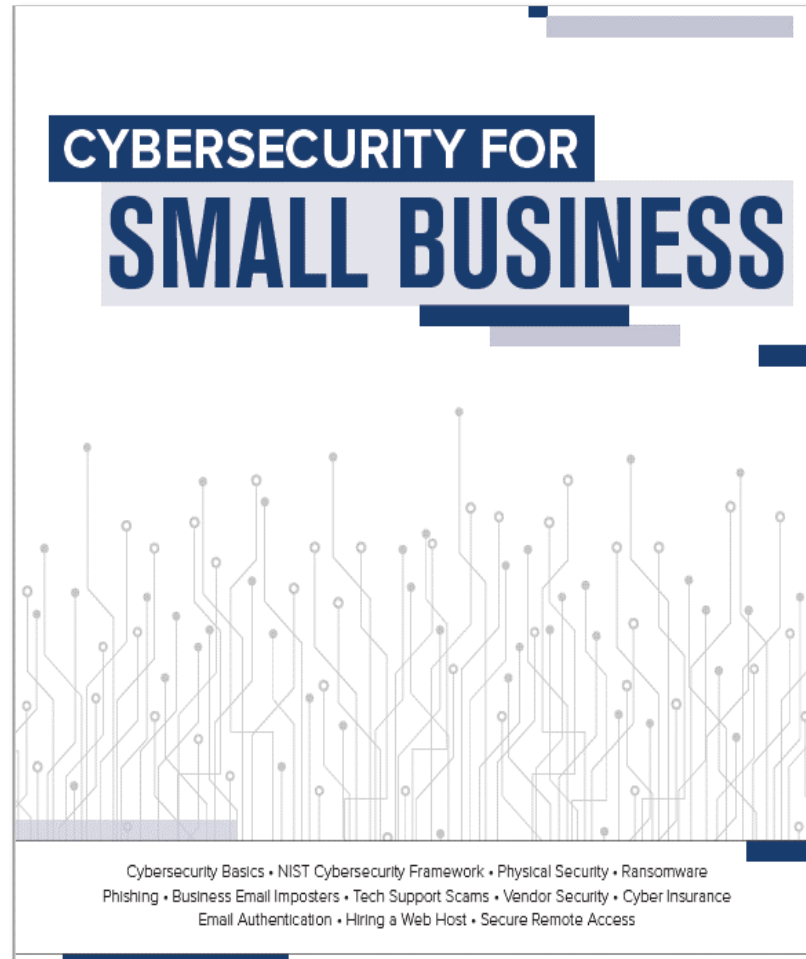
Data Breach Response: A Guide for Business

available at business.ftc.gov



Cybersecurity for Small Business

available at business.ftc.gov



FTC Staff Perspective: Web Hosts

available at business.ftc.gov

Do Web Hosts Protect Their Small Business Customers With Secure Hosting And Anti-Phishing Technologies?

STAFF PERSPECTIVE | FEBRUARY 2018

Background

During the Summer of 2017, the FTC held its first in a series of “Engage, Connect, Protect” Small Business Security Roundtables.¹ At these events, small business owners explained the challenges they face dealing with cyber threats and data security and asked the FTC for concrete advice. For many small businesses, the initial challenge they confront involves the selection of a web host and email provider. Small businesses that desire a presence on the web frequently do not have the resources or skills needed to host their own sites or to set up email accounts that use their business name as the domain name. This is especially true for businesses that are not technology-centric. A site and email accounts created and maintained by someone lacking the requisite skills may suffer from security vulnerabilities that expose the business, its customers, and others to harm such as the theft of sensitive data.

To overcome this hurdle, some companies turn to web hosting firms that market their services specifically to small businesses. These firms provide inexpensive tools and support for small businesses to establish a web presence, allowing the small business to rely on the firm’s security expertise in setting up a website and email.

The FTC’s Office of Technology Research & Investigation (OTech) examined the security features of hosting plans offered by web hosting services. OTech specifically reviewed the offerings of 11 web hosts that market their services to small businesses to examine the support they provide the small businesses in setting up SSL/TLS and email authentication technologies. The former helps ensure secure communication between a website and its visitors, and the latter helps prevent misuse of the small business’s domain by phishing schemes. Our examination found:

- Web hosts often integrate SSL/TLS setup directly into the web site creation process, helping ensure that small businesses reap the benefits of this technology.
- Support for email authentication technologies is far less extensive: few of the hosts we examined notify users of these technologies, and several do not support some technologies.

Our findings are provided in greater detail below.

¹ See <https://www.ftc.gov/news-events/blogs/business-blog/2017/07/ftc-small-businesses-gather-round>.

FTC Staff Perspective: Email Authentication

available at business.ftc.gov

Businesses Can Help Stop Phishing and Protect their Brands Using Email Authentication

STAFF PERSPECTIVE | MARCH 2017

Introduction

With subject lines such as “Suspicious Account Activity,” “Invitation to Connect,” or “Online Confirmation Required,” phishing emails can trick people into divulging usernames, passwords and other sensitive information to scam artists and harm the reputations of the businesses whose identities are spoofed. These messages often include the phished businesses’ graphics and appear to include links to the businesses’ web sites, making it difficult to tell the difference between real messages and spoofed ones. The best way to prevent people from falling for phishing messages may be to keep these scam emails from ever showing up in their inboxes.

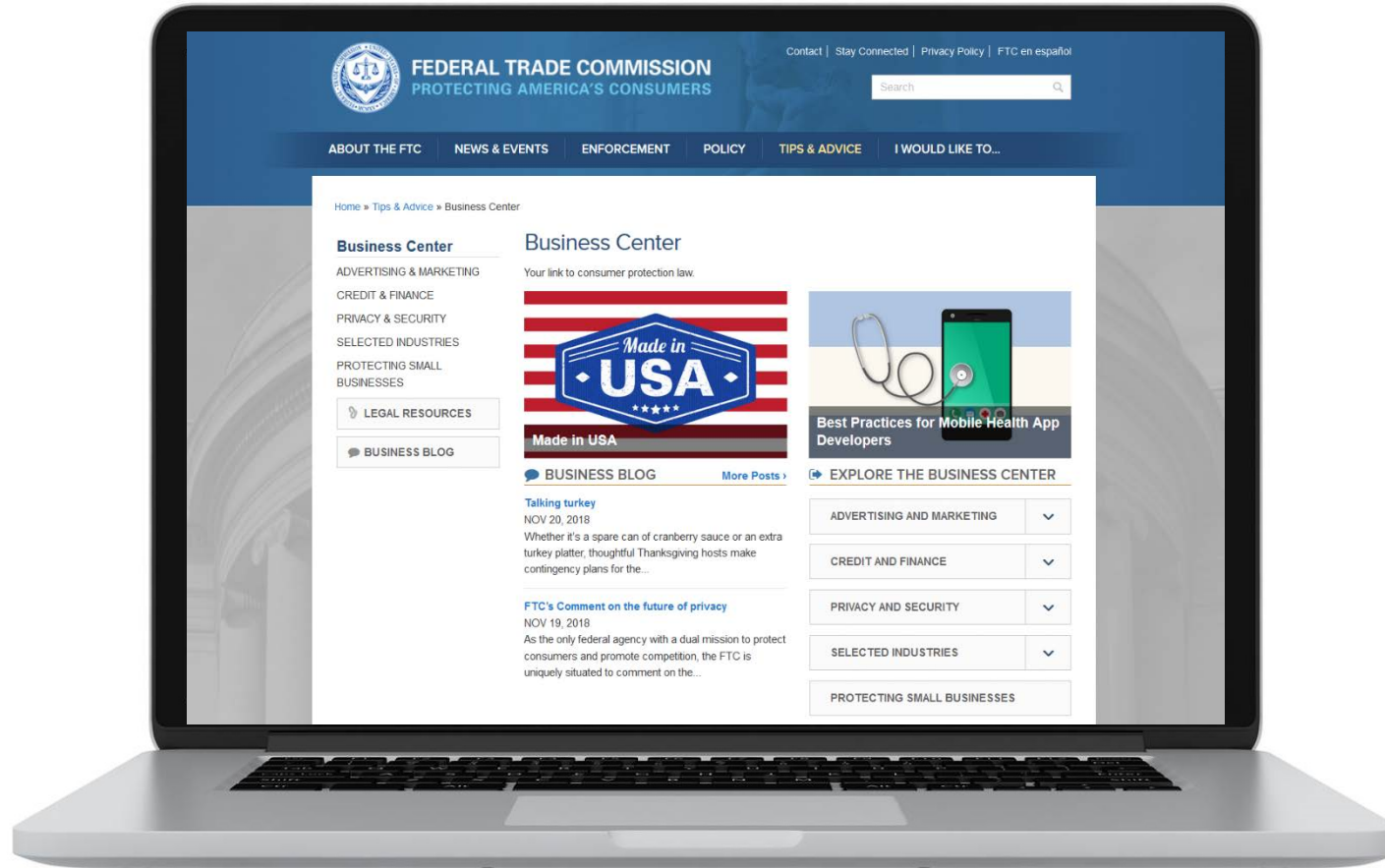
Several technical solutions exist that can help reduce the number of phishing emails reaching people. Many businesses already use some of these low cost, readily available solutions to help email providers determine the authenticity of received email. However, few of the major online businesses use the full capability of these solutions, potentially allowing many phishing emails to get through. As explained below, online businesses can play a significant role in decreasing the number of phishing emails by instructing receiving email servers to automatically reject unauthenticated emails.

In this BCP Staff Perspective, we explain that:

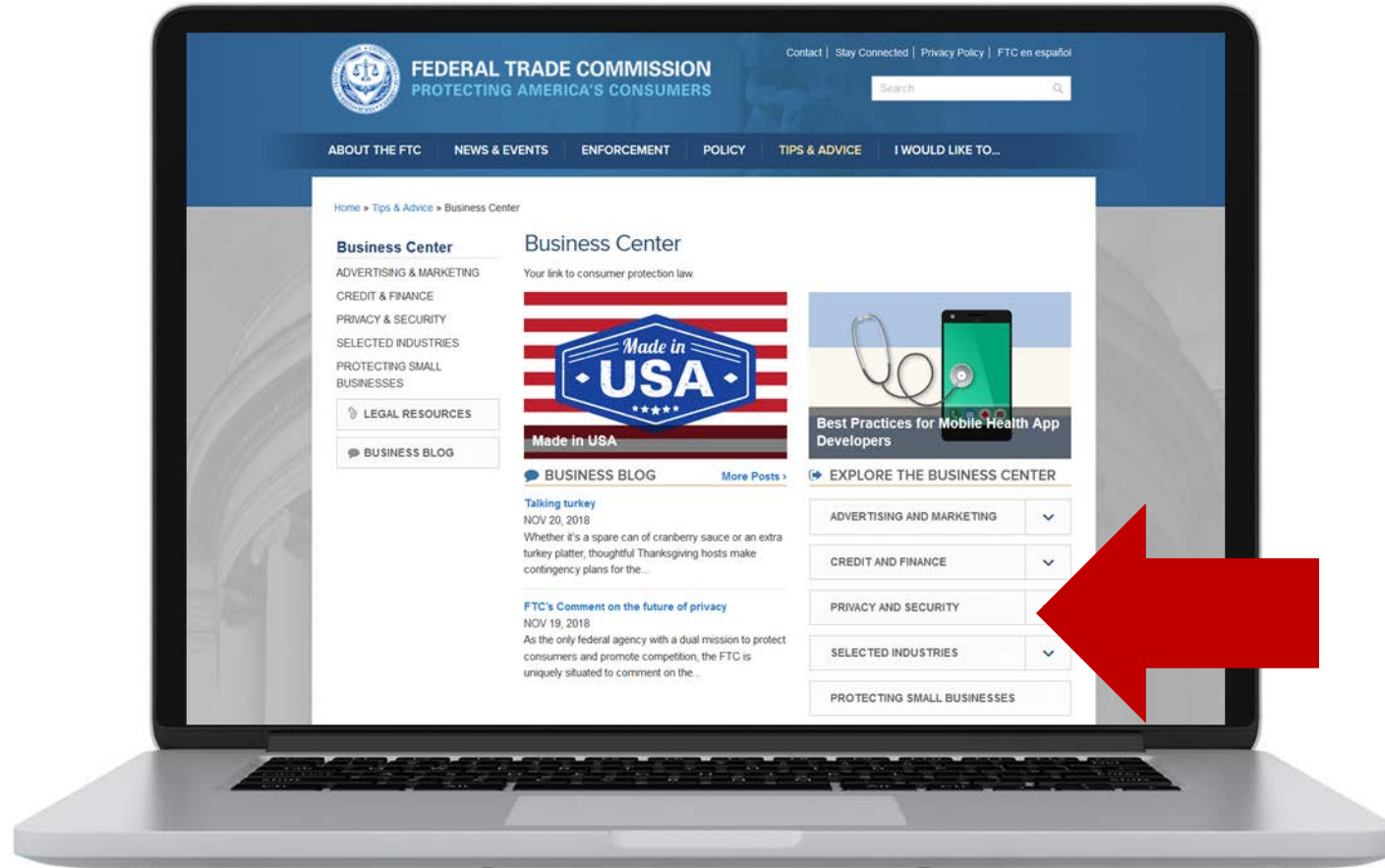
- The same design that makes email ubiquitous and simple also makes it easy to spoof email senders’ addresses and to generate phishing messages.
- A business can take two major steps to prevent its domains from being used in phishing scams:
 - Use domain level email authentication so that receiving mail servers can verify that a message that claims to be from the business actually came from a domain authorized by the business. There are two forms of domain level authentication that a business can use -- Sender Policy Framework (SPF), which allows a business to designate the IP addresses it uses to send email, and DomainKeys Identified Mail (DKIM), which allows businesses to use digital signatures to verify the authenticity and integrity of their messages.
 - Use a complementary scheme called Domain Message Authentication Reporting & Conformance (DMARC) which, among other things, enables a business to: (1) gather intelligence on how phishers and other scam artists are misusing their domains, and (2) instruct receiving email servers how to treat unauthenticated messages that claim to be from the business’s domain. In its DMARC listing, a business can instruct a receiving email server to reject unauthenticated messages

FTC BUREAU OF CONSUMER PROTECTION  FTC.GOV

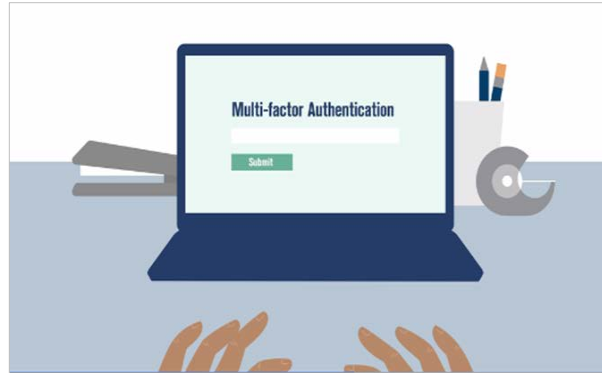
Bureau of Consumer Protection Business Center: business.ftc.gov



BCP Business Center: Privacy and Data Security Resources



Educational Videos for Business: ftc.gov/video



Ransomware - Cybersecurity for Small Business
October 15, 2018



Cybersecurity Basics for Small Business
October 15, 2018



The NIST Cybersecurity Framework and the FTC
March 9, 2017



Data Breach Response
October 13, 2016



Start with Security: Free Resources for Any Business
February 19, 2016



Keep Your Security Current
February 4, 2016



Implement Strong Password Policies
December 7, 2015



Secure Remote Access
December 2, 2015



Build Security into Development
December 2, 2015



Phishing Your Company's Good Name
January 31, 2017



Defend Against Ransomware
November 3, 2016



Stop Phishing By Using Email Authentication
November 3, 2016



Monitor Your Service Providers
January 21, 2016



Segment and Monitor Your Network
January 6, 2016



Store Information Securely
January 5, 2016



Control Access to Data
December 2, 2015



Secure Devices and Paper
November 3, 2015



Start with Security
September 4, 2015

Thank You!

**Join Us on February 12-13, 2019
For the Consumer Privacy Hearing.**

