Written Questions for the Record of Chairman Leahy
for the Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
February 11, 2014

1. **During the Committee's February 4, 2014 hearing, you testified about how American retailers can better protect consumers' sensitive financial and personal data from data breaches and cyber attacks.**

    a. **What can consumers do to better protect their sensitive personal information and financial data when making point of sale purchases? What about during online transactions?**

The FTC provides information to consumers about steps they can take to protect their personal information, both online and offline.[1] As to point of sale transactions, there is little consumers can do while shopping to detect and prevent breaches. However, they should make sure to review their billing statements afterwards and report unauthorized transactions immediately. They should also check their credit reports regularly by going to annualcreditreport.com. For online transactions, we recommend that consumers do the following: (1) keep up with security updates on browsers and operating systems; (2) make sure any website that they use to transmit financial information is encrypted, which they can tell by making sure the URL starts with https (the "s" stands for secure); and (3) create strong passwords and keep them safe. While consumers should take these measures, it is also incumbent on businesses to take reasonable steps to protect consumer information from access or use by hackers or identity thieves.

    b. **What steps should consumers take after being notified that their personal or financial information has been compromised due to a data breach or other cyber attacks?**

The FTC has long published a victim recovery guide and other resources to explain the immediate steps identity theft victims should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report; and how to protect their personal information.[2] Also, for consumers who may have been affected by the recent Target and other breaches, the FTC has posted information online about steps they should take to help protect themselves.[3] This guidance recommends that consumers review their credit card and bank statements; check their credit reports every few months; and delete phishing emails or text messages that ask consumers to confirm or provide account information.

---

[1] *See* http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure.
[2] *See* http://www.consumer.ftc.gov/features/feature-0014-identity-theft.
[3] *See* Nicole Vincent Fleming, *An Unfortunate Fact About Shopping*, FTC Consumer Blog, http://www.consumer.ftc.gov/blog/unfortunate-fact-about-shopping (Jan. 27, 2014); Nicole Vincent Fleming, *Are you affected by the recent Target hack?*, FTC Consumer Blog, https://www.consumer.ftc.gov/blog/are-you-affected-recent-target-hack (Dec. 19, 2013).

2. Has the Federal Trade Commission issued any best practices or guidance regarding how American businesses can help safeguard the privacy and security of consumers' sensitive personally identifiable information? If so, please briefly explain.

The FTC widely disseminates its business guide on data security,[4] along with an online tutorial based on the guide.[5] These resources are designed to provide a variety of businesses – and especially small businesses – with practical, concrete advice to be used as they develop data security programs and plans for their companies. The Commission has also released guidance directed towards a non-legal audience regarding basic data security issues for businesses.[6] For example, because mobile applications ("apps") and devices often rely on consumer data, the FTC has developed specific security guidance for mobile app developers as they create, release, and monitor their apps.[7] The FTC also publishes business educational materials on specific topics – such as the risks associated with peer-to-peer ("P2P") file-sharing programs and companies' obligations to protect consumer and employee information from these risks[8] and how to properly secure and dispose of information on digital copiers.[9]

3. The collection and retention of consumer data is also a significant privacy issue for many American consumers and businesses.

a. What are the FTC's views on whether consumers should be notified about commercial data collection and retention practices?

Companies should be transparent about their data practices and should provide simplified notice to consumers of their data practices – where possible on a just-in-time basis – to the extent such practices are inconsistent with the context of an interaction. More comprehensive notices of privacy practices should also be provided and are important, both for consumers who are interested in comparing companies' practices and for regulators, consumer advocates, and other watchdog organizations who can hold companies accountable. It is important for these comprehensive privacy notices to provide a clear and concise description of the company's data collection and use practices. Notice aside, companies should also follow principles of privacy by design, such as limiting their collection of consumers' information to the extent they need it in order to fulfill a legitimate business purpose. They should assess how long they need to store consumers' information in order to meet these purposes, and dispose of the information when it

---

[4] *See Protecting Personal Information: A Guide for Business*, *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

[5] *See Protecting Personal Information: A Guide for Business (Interactive Tutorial)*, *available at* http://business.ftc.gov/multimedia/videos/protecting-personal-information.

[6] *See generally* http://www.business.ftc.gov/privacy-and-security/data-security.

[7] *See Mobile App Developers: Start with Security* (Feb. 2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

[8] *See Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), *available at* http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.

[9] *See Copier Data Security: A Guide for Business* (Nov. 2010), *available at* http://business.ftc.gov/documents/bus43-copier-data-security.

is no longer needed. All of these best practices are described in greater detail in the Commission's Privacy Report.[10]

b. In your view, should businesses that collect and retain consumer data allow their customers to "opt out" of these data collection and retention activities?

The FTC has encouraged companies to provide simpler and more streamlined choices to consumers about their data practices. In the Commission's Privacy Report, we stated that companies need to provide choice before collecting and using consumers' data for practices that are inconsistent with the context of the consumer's interaction with the business. In these instances, consumers should have the ability to make informed and meaningful choices at a "just-in-time" point.[11] Choice is not necessary for data practices that are consistent with the context of the transaction, the company's relationship with the consumer, or as required or specifically authorized by law. For example, companies need not give consumers choices about collecting their address in order to deliver a product.

4. In your experience, are "point of sale" or online commercial transactions most likely to result in a data breach involving consumer data?

We have seen no clear trend as to the source or type of data breach. Reported breaches range from lost laptops to hacking, to inadequate website security, to corrupt insiders, to misplaced shipments.

This is precisely why we have encouraged companies to implement reasonable information security practices to protect consumers' sensitive information. The Commission's Gramm-Leach-Bliley Safeguards Rule provides a good roadmap as to the procedures and basic elements necessary to develop a sound security program. Although it applies only to non-bank financial institutions, we believe it provides valuable guidance to other companies as well.

5. Do you anticipate that we will witness an increase in "point of sale" data breaches given the recent trend of data breaches involving American retailers?

I am not in a position to predict whether we will witness an increase in point of sale data breaches given recently announced breaches involving American retailers. However, reports of data breaches affecting American consumers continue to rise. This is precisely why the Commission has unanimously called for federal legislation that would (1) strengthen existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.

---

[10] *See Protecting Consumer Privacy in an Era of Rapid Change* (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[11] *Id.* at 48-50.