Responses to Questions for the Record
Delara Derakhshani, Policy Counsel, Consumers Union
February 11, 2014

1. *During the Committee's February 4, 2014 hearing, there was a great deal of discussion about how American retailers, and other industries, can better protect 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 purchases in a store or online?*

In our June 2013 issue of *Consumer Reports,* we identified several steps that consumers can take to help protect their personal information online, such as safeguarding the computers and mobile devices that they use to make online purchases. Smartphones, for example, may contain a great deal of personal information about you – including your contacts, e-mails, and bank account information – yet our research suggests that many Americans are not taking sufficient measures to adequately protect their smart phones. We've advised consumers to use screen locks and strong passcodes, back up their data, make sure their security software is up-to-date, and install apps to locate a missing phone and remotely erase data. Before selling or recycling a phone, consumers should also delete any sensitive data from the phone, remove any memory cards, and restore the phone's original factory settings. And the same thing applies to disposing of an old PC or laptop: consumers should make sure a hard drive is properly erased before recycling, donating, or disposing of a computer.

    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 cyberthreat?*

Consumers should regularly review their bank accounts and credit and debit cards to be on the look out for fraudulent use. Consumers who spot any suspicious charges should report them immediately to their financial institutions. For additional protection, consumers can also replace their debit and credit cards, which will stop fraud on those accounts if the account number is what has been compromised. Consumers can also set up account alerts, so that their debit or credit card provider sends an e-mail or text if a transaction occurs over a specified limit.

In the event of a breach, some companies may offer free credit monitoring services. Credit monitoring will catch the opening of new accounts, but it is not designed to catch is fraudulent use of existing accounts. Consumers may want to take advantage of free credit monitoring service, so long as they understand its limitations. For example, credit monitoring won't immediately catch fraudulent transactions on your current credit, debit, and prepaid cards, so consumers affected by a breach still need to be vigilant in checking their existing accounts. Furthermore, we have advised consumers to be aware of when any free monitoring period ends, so that they aren't automatically charged for continuing such services. Finally, in order for credit

monitoring to be most effective, consumers should obtain credit reports from all three credit bureaus, not just one, because the information from each of the three bureaus can be different.

Consumers may also want to place a fraud alert or security freeze on their credit reports. Setting up a fraud alert requires anyone who would be extending you new credit to take extra steps to verify your identity. A fraud alert is a less drastic step than a security freeze, which stops new creditors from accessing a credit report. If there is a chance that a data breach includes your Social Security number, then a freeze would be more effective than a fraud alert to protect yourself from this kind of scam.

It's also possible, however, that thieves might also use stolen data to help them obtain your Social Security number, which they could then use to open new accounts in your name. For this reason, consumers should not give out personal information unless they have independently verified the legitimacy of any messages they receive on behalf of a bank or other institution.

It's worth noting that in many states, there is a cost attached to security freezes. When you want to engage in a legitimate transaction, you may need to temporarily lift and then re-impose the security freeze, which can cost money. In some states, you have to provide a report from the police, motor vehicles department, or some other agency in order to obtain a freeze at no cost. Consumers should check credit bureaus' websites to find out what is required for freezes and temporary lifts.

2. *Do online purchases and transactions pose any additional privacy risks for consumers? Please explain.*

Online purchases and transactions can pose a number of privacy risks for consumers. Anything from weak passwords to shady websites to insecure wireless connections put consumers at risk. Consumer Reports and Consumers Union continues to seek to educate consumers about these risks through our various print and online publications.

We are also concerned about public Wi-Fi networks that many consumers use to make financial transactions. Our June 2013 issue of *Consumer Reports* estimated that thirteen million users engaged in financial transactions at wireless hotspots, but consumers are not always aware that this information can be intercepted. We have advised against conducting transactions over insecure Wi-Fi networks, as this can expose your credit card numbers, user information, passwords, and other information to anyone who has access to that network.

We have recommend a number of tips to consumers to protect themselves in these instances, including turning off Wi-Fi and switching their phone to 3G/4G mode before sending or receiving sensitive data. We have also suggested the use of virtual private networks, which encrypt data before sending. Finally, we have suggested that consumers who use an app to conduct a transaction check the app's privacy policy to see how it handles sensitive information being transmitted wirelessly.