ConsumersUnion
POLICY & ACTION FROM CONSUMER REPORTS

STATEMENT OF

DELARA DERAKHSHANI
CONSUMERS UNION

BEFORE THE

UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

ON

"PRIVACY IN THE DIGITAL AGE: PREVENTING DATA BREACHES AND COMBATING CYBERCRIME"

FEBRUARY 4, 2013

Chairman Leahy, Ranking Member Grassley, and esteemed members of the Committee. Thank you for the opportunity to testify before you today about data breaches. My name is Delara Derakhshani, and I serve as policy counsel for Consumers Union, the policy and advocacy arm of Consumer Reports.

This past December – at the height of the holiday shopping season – 40 million unsuspecting consumers learned that criminals may have gained unauthorized access to their credit and debit card numbers. Subsequently, 70 million more Target customers learned that personal information such as names, home addresses and telephone numbers may have also fallen into the hands of suspected criminal hackers. We now also know of similar breaches at other retailers: Neiman Marcus confirmed unauthorized access to payment data, and – most recently – Michael's has reported that it is investigating whether a similar breach occurred. The press is reporting that this may be the tip of the iceberg because versions of the malware that was reportedly used in the Target and Neiman Marcus cyberattacks was sold to cybercriminals overseas.

This is truly disturbing. The threats from such breaches are real – and they are serious. As Consumer Reports and Consumers Union have reported with regularity in our publications, consumers who have their data compromised in a large-scale security breach are more likely to become victims of identity theft or fraud. Although federal consumer protection lending laws and voluntary industry practices generally protect consumers from significant out-of-pocket losses, consumers, policymakers, and regulators should take this threat seriously – not only to prevent fraudulent charges which in the end could wind up coming out of the pockets of the retailers, but also because a security breach exposes consumers to unpredictable risks that their personal data will be used without their authorization and for nefarious purposes.

Then there are the very practical and time-consuming concerns for consumers whose personal data has been breached. Consumers have to cancel cards, and must monitor their credit reports and continue to do so in the future. Even though millions have not yet experienced a problem, the threat and uncertainty are there. Of particular concern are debit cards which carry fewer legal protections. While consumers might not ultimately be held responsible if someone steals their debit card and pin number, data thieves can still empty out consumers' bank accounts and set off a cascade of

bounced checks and late fees which victims will have to settle down the road.

Clearly, the burden is being put on consumers to be vigilant to prevent future fraudulent use of their information.

What can happen to the data after it's stolen is disconcerting, to say the least. Sometimes, data is resold to criminals outside of the country. Other times, it is used to create counterfeit credit cards or debit cards with direct access to your checking account. Even if you do not wind up becoming a victim of identity theft or have your card used for fraudulent purposes, the result is decreased consumer confidence in the marketplace and uncertainty with the realization that your private financial data is in the ether, and could one day be accessible to individuals for any purpose whatsoever.

Furthermore, in the wake of these breaches, a number of scam artists are trying to take advantage of the situation. What is happening is that scammers are trying to prey on concerns about compromised data. These scammers are attempting to gather consumers' personal and credit information – sometimes through a method called "phishing." We have urged consumers to verify the authenticity of any breach-related messages they receive, and to be wary of emails and phone calls offering identity theft or fraud protection.

When Consumers Union learned of the breach, we wrote to the CFPB, urging them to investigate the matter and for increased public disclosure. Just last week, Attorney General Eric Holder confirmed that the Department of Justice is also investigating the matter. We know lawmakers have urged the Federal Trade Commission to investigate as well. We are grateful that the federal agencies – and State Attorneys General – are on the case, so that we can get to the bottom of who did this and how it happened. And together we can formulate policies and procedures to prevent data breaches from occurring in the future.

Consumers Union and Consumer Reports have also provided consumers with a number of tips to protect themselves – such as closely monitoring their accounts, checking their financial statements frequently, and notifying their financial institutions of any suspicious card activity immediately. For extra protection, consumers can replace credit card numbers as well as debit cards and PIN numbers. We explained that consumers affected by a breach can go online and request a 90-day fraud alert on their credit reports with the

three national credit bureaus – Equifax, Experian, and TransUnion – so that they can be notified if thieves try to open up a new credit account in their name. This type of new account fraud is rare and requires a Social Security number – and there's no evidence at this time that hackers have access to consumers' Social Security numbers. But consumers should know that this additional protection is available to them if they want it. Consumers may also want to place a security freeze on their credit report – which blocks access to your credit file by lenders who don't already do business with you. Finally, we have urged consumers not to waste $120 to $300 a year on so-called identity theft protection services. As we've pointed out, consumers can protect themselves for little or nothing. Some of these services use deceptive marketing to sell overpriced and useless products to consumers.

Target and affected retailers are also offering consumers credit monitoring. We believe there are some things that consumers should consider before they enroll in these services. First, consumers should recognize that these services are only free for a year. Although Target assures consumers that they will not be automatically re-enrolled, consumers may get sales solicitations when the free period ends. Second, as some consumer advocates have pointed out, in order to sign up, consumers have to agree to mandatory arbitration, which means that they waive their right to go to court should a dispute arise.

It is important to point out that we should also focus on what needs to be done to help avoid data breaches in the first place. The credit cards and debit cards most Americans use are surprisingly vulnerable to fraud, relying on decades-old technology that makes them susceptible. American credit and debit card data are usually stored unencrypted on a magnetic stripe on the back of each card. Thieves can cheaply and easily "skim" the data off of this magnetic stripe when a credit or debit card is swiped and create a counterfeit card that can access a cardholder's account at an ATM.

Many other countries have shifted or are in the process of shifting to what is known as EMV "smart cards" – or chip and pin technology, which utilizes multiple layers of security – including a computer chip in each card that stores and transmits encrypted data, as well as a unique identifier that can change with each transaction. Cardholders also enter a PIN to authorize transactions. Total fraud losses dropped by 50 percent and card counterfeiting fell by 78 percent in the first year after EMV smart cards were introduced in France in 1992. The United States has lagged behind because

replacing all payment cards, updating ATMs to accept the new cards, and updating the terminals in retail stores all cost money. Some financial institutions have indicated that they will switch over to this new technology in the next few years. We need a stronger commitment from all stakeholders to adopt this technology sooner rather than later. We believe it is money well-spent, and it is a penny-wise pound-foolish philosophy to wait any longer, particularly when the burden of guarding against harm following a breach falls most squarely on the shoulders of innocent consumers whose data was compromised.

Policymakers must also take action to encourage investments in new technology to help financial institutions tighten up the own security to help prevent fraud. We need to make sure that we don't fall further behind the rest of the world in fraud protection.

These incidents reinforce just how timely and relevant this Committee's efforts are to guard against data breaches and to quickly help consumers should a breach occur. We appreciate the efforts of Chairman Leahy and the Committee on data breaches, and we recognize the long history of involvement in the topic.

The current legislation introduced by the Chairman, the Personal Data Privacy and Security Act of 2014, would encourage companies to be proactive about safeguarding the data that is entrusted to them.

We applaud the sponsors' desire to ensure that consumers are notified when a breach occurs. We believe that the sooner consumers know that their data has been compromised, the sooner they can take steps to protect themselves. We would therefore urge the Committee to consider shortening the timeline for notification from the 60 days currently in the bill to require more immediate notification. We appreciate the bill's provisions to require companies to identify security vulnerabilities, and periodically assess whether their data privacy and security programs are able to address current threats.

We are also pleased that the bill grants enforcement power to both the Federal Trade Commission and State Attorneys General. The enforcement provisions of the bill are a crucial element of a data security framework, and as we have stated previously – we strongly believe that State Attorneys General must be involved in such enforcement. State Attorneys General

have been at the forefront of notice and data breach issues and have played an invaluable role in the efforts to address identity theft and data breaches.

In testimony to Congress on this matter, Consumers Union has repeatedly pointed out that the strongest state notice of breach laws do not require a finding of risk before requiring notification to consumers. Although Consumers Union would prefer that consumers receive notification anytime their personal information is compromised – if there is to be a standard for risk, then Consumers Union would prefer the approach taken by this bill – in which the risk is considered an exemption rather than an affirmative trigger. Under this exemption approach, insufficient information about the level of risk does not eliminate a company's obligation to tell consumers about the breach.

Nevertheless, we would like to strengthen some provisions in the bill, including those related to pre-emption. We want to make sure that any national standard results in strong, meaningful protections for consumers – but that any federal standard does not tie the hands of states or limit their ability to adopt additional protective measures for consumers. Our organization supported the California breach law passed in 2002 and enacted in 2003, and we have a long history of working with state legislatures to pass initiatives that would protect consumers. As a result, we would certainly urge that any federal law addressing data breach and notification set out a floor – not a ceiling – allowing states the freedom to innovate in order to address new threats to consumers.

In closing, thank you for the opportunity to speak before you today. We appreciate the Committee's interest in data security, and we encourage policymakers and regulators to continue to press for responsible data security practices with a new urgency. We all want to ensure consumer confidence in the marketplace. Data breaches undermine that confidence and place unfair burdens on consumers. We look forward to working with the Committee and other stakeholders to make sure that consumers – and their information – are protected adequately. Thank you.