Prepared Statement
Illinois Attorney General Lisa Madigan
"Protecting Consumer Information: Can Data Breaches Be Prevented?"

Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy & Commerce
United States House of Representatives

February 5, 2014

I. INTRODUCTION

Chairman Terry, members of the Subcommittee, thank you for inviting me to testify today about this important issue. Addressing data breaches and preventing them is critical to our financial security and our economy. Over the past decade, we have faced an epidemic of data breaches that has affected almost every American and has inflicted billions of dollars of damage to our economy.

The most frustrating aspect of this problem is that data breaches are not new. No one is surprised to hear the latest data breach reported in the news. We have become too accustomed to their occurrence, and it is time the government and the private sector take serious, meaningful actions to curb this growing problem. As we become more dependent on technology in our everyday lives, breaches will increasingly affect more consumers and, in the process, do more damage.

To assist the Subcommittee, I will explain:

- the impact data breaches have on consumers;
- the role the states play in responding to breaches;
- the data security lapses we have seen in private companies; and
- the steps the private sector and the government can take to prevent future breaches.

II. IMPACT ON CONSUMERS

Since 2005, there have been over 4,000 data breaches nationally and over 733 million records compromised.[1] In the last year alone, the number of complaints my office has received on data breaches has jumped more than 1,000%.[2] Since 2006, identity theft has been the highest or second highest source of complaints to my office every year, totaling 31,100 complaints.[3] When data breaches occur, consumers are harmed primarily for two reasons:

- they face the likelihood of unauthorized charges on their existing accounts; and
- they are much more likely to become victims of identity theft.

A. Fraud on Existing Accounts

When financial information is compromised, consumers must constantly monitor their financial accounts for any unauthorized charges. Once a consumer does discover unauthorized charges, cleanup requires:

- notifying their credit and debit card issuers of the compromised cards;
- closing accounts, canceling cards, and waiting for new cards to arrive; and
- for consumers with automatic bill pay, alerting companies about the new account numbers to prevent late fees.

[1] Figure includes publicly reported data breaches between 2005 and 2014 compiled by Privacy Rights Clearinghouse (663,182,386 as of February 3, 2014) in addition to the publicly reported 70 million records compromised in the 2013 Target Data Breach. *See* Privacy Rights Clearinghouse, Chronology of Data Breaches, *available at* http://www.privacyrights.org/data-breach/new; Press Release, Target Corp., "Target provides Update on Data Breach and Financial Performance," *available at* http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.

[2] In 2012 the Illinois Attorney General's office received 34 complaints regarding data breaches, compared to 605 in 2013.

[3] *See* Press Release, Office of Illinois Attorney General Lisa Madigan, "Top Ten Consumer Complaints" for 2006, 2007, 2008, 2009, 2010, 2011, and 2012, *available at* http://www.illinoisattorneygeneral.gov/consumers/index.html.

These issues are more than mere inconveniences. Consumers and banks can also easily miss unauthorized charges on accounts. And when that happens, the consumer will be responsible for the fraud.

Everyday my office contends with the enormous amount of time, effort, and stress consumers face when they attempt to sort out the impact of data breaches involving their existing financial accounts.

B. Identity Theft

The amount of money consumers lose because of identity theft is sobering. In 2012 alone, $21 billion was lost to identity theft.[4] The fraud takes a variety of forms. Identity theft most commonly affects consumers' financial accounts. But identity thieves also:

- open fake utility accounts;
- obtain prescription drugs and medical treatments using others' identities;
- receive government benefits using compromised consumer data; and
- target children because of their clean credit history.

Since 2010, my office has assisted nearly 350 minors who have been victims of identity theft.[5] We have helped shut down hundreds of fraudulent accounts, which were opened using the identities of children.

Victims of identity theft can spend months contacting banks, credit card companies, credit reporting agencies, public utility companies, and the police to report instances of fraud and to restore their credit. These victims can also be prevented from fully participating in our

[4] Javelin Strategy & Research, *How Consumers can Protect Against Identity Fraudsters in 2013*, 4 (Feb. 2013). This statistic includes all types of identity theft, not just identity theft related to data breaches.

[5] Social Security Number Protection Task Force, *Report to Governor Pat Quinn, Attorney General Lisa Madigan, Secretary of State Jesse White, and Illinois General Assembly*, 6 (Dec. 31, 2013).

economy, meaning their entire lives can be put on hold. An identity theft can prevent a consumer from purchasing a home or finding a place to rent. All this can happen because a consumer shared their sensitive data with a business, a hospital, or the government.

III. Role of the States

The states have seen firsthand how damaging this is for consumers. In response, my office created a dedicated Identity Theft Unit and Hotline in 2006.[6] Since then, we have received more than 40,000 requests for assistance and have helped thousands of Illinois residents. The unit and hotline are staffed with experts who walk consumers through the lengthy and complicated process they face when reporting fraud and restoring their credit. We have also developed a fifty-six page, comprehensive Identity Theft Resource Guide for Illinois residents to use when facing identity theft. [7]

The states began focusing in earnest on data breaches in 2005 when ChoicePoint, a very large data broker, experienced a significant data breach that harmed thousands of consumers.[8] In response, Illinois passed a data breach law to ensure companies notify consumers when their

[6] Press Release, Office of Illinois Attorney General Lisa Madigan, "Madigan Announces Activation of ID Theft Hotline; Help Line is First of Its Kind in the Nation" (Feb. 7, 2006).

[7] Identity Theft Resource Guide, *available at* http://www.illinoisattorneygeneral.gov/consumers/Identity_Theft_Resource_Guide.pdf.

[8] Press Release, Office of Illinois Attorney General Lisa Madigan, "Attorney General Madigan Reaches Agreement with ChoicePoint" (May 31, 2007).

sensitive information is compromised.[9] Since then, nearly every other state has passed a law requiring companies to notify consumers of data breaches that compromise sensitive data.[10]

My office also leads the National Association of Attorneys General (NAAG) Privacy Working Group, which consists of more than forty states. We convene regularly to discuss and investigate privacy issues, including data breaches that affect consumers in multiple states. With respect to the recent data breaches, my office, along with the Connecticut Attorney General's office, is leading multi-state investigations into the breaches that have impacted millions of customers of Target, Neiman Marcus, and Michaels.[11]

While I cannot comment on the specifics of an ongoing investigation, I can explain why we conduct these investigations in the first place:

---

[9] Illinois Personal Information Protection Act (PIPA), 815 Ill. Comp. Stat. 530/1 et. seq. (2006). PIPA requires notification to a consumer when an unauthorized acquisition of computerized data compromises the security, confidentiality, or integrity of personal information maintained by the data collector. Personal information means an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data element are not encrypted or redacted: social security number, driver's license number or State identification card number, account number or credit card number, or account number or credit card number in combination with any required security code, access code, or password. Notice to consumers must occur in the most expedient time possible and without unreasonable delay.

[10] Alaska Stat. §45.48.010 et seq.; Ariz. Rev. Stat. §44-7501; Ark. Code §4-110-101 et seq.; Cal. Civ. Code §§1798.29, 1789.80 et. seq.; Colo. Rev. Stat. §6-1-716; Conn. Gen Stat. 36a-701(b); Del. Code tit. 6, §12B-101 et seq.; Fla. Stat. §817.5681; Ga. Code §§10-1-910, -911, -912; § 46-5-214; Haw. Rev. Stat. §487N-1 et. seq.; Idaho Stat. §§28-51-104 to -107; 815 ILCS 530/1 to 530/25; Ind. Code §§24-4.9 et seq., 4-1-11 et seq.; Iowa Code §715C.1, 715C.2; Kan. Stat. 50-7a01 et. seq.; La. Rev. Stat. §51:3071 et seq.; Me. Rev. Stat. tit. 10 §§1347 et seq.; Md. Code, Com. Law §14-3501 et seq.; Mass. Gen. Laws §93H-1 et seq.; Mich. Comp. Laws §§ 445.63, 445.72; Minn. Stat. §§325E.61, 325E.64; Miss. Code § 75-24-29; Mo. Rev. Stat. §407.1500; Mont. Code §§30-14-1704, 2-6-504; Neb. Rev. Stat. §§87-801, -802, -803, -804, -805, -806, -807; Nev. Rev. Stat. 603A.010 et seq.; N.H. Rev. Stat. §§359-C:19, -C:20, -C:21; N.J. Stat. 56:8-163; N.Y. Gen. Bus. Law §899-aa; N.C. Gen. Stat §75-65; N.D. Cent. Code §51-30-01 et seq.; Ohio Rev. Code §§1347.12, 1349.19, 1349.191, 1349.192; Okla. Stat. §74-3113.1, §24-161 to -166; Oregon Rev. Stat. §646A.600 et seq.; 73 Pa. Stat. §2303; R.I. Gen. Laws §11-49.2-1 et seq.; S.C. Code §39-1-90; Tenn. Code §47-18-2107; Tex. Bus. & Com. Code §521.002, 521.053; Utah Code §§13-44-101, -102, -201, -202, -310; Vt. Stat. tit. 9 §2430, 2435; Va. Code §18.2-186.6, §32.1-127.1:05; Wash. Rev. Code §19.255.010, 42.56.590; W.V. Code §§46A-2A-101 et seq.; Wis. Stat. §134.98 et seq.; Wyo. Stat. §40-12-501 to -502; D.C. Code §28- 3851 et seq.; Guam 9 GCA § 48-10 et. seq.; 10 Laws of Puerto Rico §4051 et. seq.; V.I. Code §2208. *See* State Security Breach Notification Laws, Nat'l Conference Of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Jan 21, 2014).

[11] Bloomberg, "Connecticut Attorney General Probing Neiman Marcus Breach," Jan. 14, 2014, *available at* http://www.bloomberg.com/news/2014-01-13/connecticut-attorney-general-probing-neiman-marcus-breach.html.

- to confirm that companies notified their customers within a reasonable timeframe and satisfied the requirements of Illinois law and other states; and
- to ensure that companies suffering breaches took reasonable steps to protect their customers' sensitive data from disclosure.

IV. Weaknesses in Security Systems

During past investigations, we have repeatedly found instances where companies failed to take basic steps to protect consumer data. The notion that companies are already doing everything they can to prevent data breaches is false. We have found instances where companies:

- failed to encrypt consumer data;
- failed to install updated security patches for software; and
- needlessly stored sensitive consumer data that was not necessary for any business purpose

The recent breaches have also led to discussions about security technology that was available, but not deployed, allegedly because of the cost. It is embarrassing that our country is behind most of the world when it comes to the security of our payment networks. It is past time for the private sector to take data security seriously.

V. Next Steps for the Private Sector and the Government

Based upon our experiences at the state level, I recommend that Congress take the following actions.

First, pass data security legislation that does not preempt state law and requires companies to:

- adopt reasonable data security practices;

- only collect information from consumers that is necessary for legitimate business needs;
- delete consumer data as soon as it is no longer needed; and
- notify consumers in a timely manner when a data breach occurs.

Second, Congress should also recognize that the federal government should assist the private sector in the same manner it already assists in other critical areas. For that reason, Congress should give an agency the responsibility and authority to investigate large, sophisticated data breaches in a similar manner that the NTSB conducts investigations of aviation accidents.

Finally, please remember that the states have been on the front lines of this battle for a decade. Illinois residents understand the important role my office plays and they are not asking for our state law to be preempted. But they are asking why companies are not doing more to protect their personal and financial information and prevent these breaches from occurring in the first place.

I am happy to answer any questions you have.

Thank you.