Committee on Science, Space and Technology
United States House of Representative

Dr. Larry A. Ponemon: Testimony

My name is Dr. Larry Ponemon and I am the founder and chairman of Ponemon Institute. Our Institute was established in 2002 and we are headquartered in Traverse City, Michigan. Our mission is to advance responsible information management among business and government through independent research on privacy, data protection, information security and information ethics. Our studies are widely disseminated and have been cited in more than 50 countries across the globe.

My background represents nearly 40 years of professional experience and knowledge about privacy, compliance and information security. My career started in the Navy during the Vietnam War era. I earned a Ph.D. in accounting ethics from Union College and a Masters degree from Harvard University. Prior to the founding of our Institute, I was a tenured university professor, the executive director of information ethics at KPMG and the global managing partner for compliance risk management at PriceWaterhouseCoopers. I have served on the Advisory Committee for Online Access and Security for the U.S. Federal Trade Commission and the Data Privacy and Integrity Advisory Committee (DPIAC) for the U.S. Department of Homeland Security. I also had the privilege of serving on various privacy advisory committees at the U.S. state level.

I understand that the purpose of my testimony today is to provide assistance in understanding the potentially devastating consequences of a data breach to individuals, households and society. For more than a decade, we have studied the cost and consequences of data breach through extensive consumer studies as well as benchmark research on the privacy and data protection practices of companies in the private and public sectors. In the area of healthcare, we have conducted four annual studies on medical identity theft and patient privacy and security protections within hospitals and clinics. We also survey consumers on

their perceptions about the organizations they trust the most to protect their privacy. Among U.S. federal government sector, we are pleased to report that consumers consistently rank the United States Postal Service as the most trusted government entity for privacy. Other notable departments include the IRS, Census Bureau and Veteran's Administration.

Today I have been asked to testify about the possibility of identity theft on the Healthcare.gov website and the potential consequences to the American public. Identity theft and medical identity theft are not victimless crimes and affect those who are most vulnerable in our society – such as the ill, elderly and poor.

Beyond doing numerous empirical studies on this topic, this is an issue that really struck home. Last year my 88-year-old mother who lives in Tucson, suffered a stroke. She was rushed to the hospital and admitted. Unbeknownst to her, an identity thief was on the premises and made photocopies of her driver's license, debit card and credit card she had in her purse. The thief was able to wipe out her bank account and there were charges on her credit card amounting to thousands of dollars. In addition to dealing with her serious health issues, she also had to cope with the stress of recovering her losses and worrying about more threats to her finances and medical records.

The situation with my mother in the hospital and those who are sharing personal information on the healthcare.gov website are not dissimilar. My mother had a reasonable expectation that the personal information she had in her wallet would not be stolen – especially by a hospital employee. Those who visit and enroll in healthcare.gov also have an expectation that the people who are helping them purchase health insurance will not steal their identity. They also have a reasonable expectation that all necessary security safeguards are in place to prevent cyber attackers or malicious insiders from seizing their personal data.

In my opinion, the controversy regarding security of the healthcare.gov website is both a technical and emotional issue. In short, security controls alone will not ease the public's concerns about the safety and privacy of their personal information. Based on our research, regaining the public's trust will be essential to the ultimate acceptance and success of this important initiative.

Following are some key facts that we have learned from our consumer research on privacy, data protection and information security:

— First, the public has a higher expectation of the protection of their personal information when using or browsing government websites such as the USPS or IRS then when accessing commercial websites such as Amazon.com or ebay.com.
— Second, the loss of one's identity can destroy a person's wealth and reputation. Further, the compromise of credit and debit cards drives the cost of credit up for everyone, thus making it more difficult for Americans to procure goods and services.
— Third, medical identity theft negatively impacts the most vulnerable people in our nation. Beyond financial consequences, the contamination of health records caused by imposters can result in health misdiagnosis and in extreme cases could be fatal. Because there are no credit reports to track medical identity theft, it is nearly impossible to know you have become a victim.

Based on our Institute's research, I would like to recommend a three-part approach to raising the trust and confidence of Americans when using healthcare.gov to buy health insurance.

- First, is accountability. It is important to demonstrate to the public that the government is accountable for the security of the information and can be trusted. This translates into standards that do not just meet basic practices but exceeds them to ensure the website is safe and secure. As an example,

one requirement should be to encrypt all personal data at rest in backend systems.

- Second, is ownership by the CEO. In this case it is the president of the United States who should take ownership of the website and ensure good security and privacy practices are met as a priority.

- Third, is independent verification or audit of the website to ensure all areas and underlying systems meet high security standards.

Thank you for the opportunity to be part of this hearing.

Respectfully,

LA. Ponemon

Dr. Larry Ponemon
Founder & Chairman
Ponemon Institute