

**Prepared Statement of Jeanette Fitzgerald
General Counsel
Epsilon Data Management, LLC**

**Before the House Committee on Energy & Commerce
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives**

June 2, 2011

Chairman Bono Mack, Ranking Member Butterfield, and distinguished members of the Subcommittee, my name is Jeanette Fitzgerald and I am the General Counsel for Epsilon Data Management. Thank you for inviting me to present Epsilon's testimony on data security.

Epsilon has been asked to participate in this hearing because it has been the victim of a criminal hacking incident. Since the incident occurred, Epsilon has worked closely with the Secret Service to identify the criminals who engaged in this malicious attack. Although it is ongoing, that investigation to date has confirmed that only email addresses and, in some cases, first and last names were affected by the attack. There is currently no evidence that any other data the company maintains were compromised.

We appreciate the opportunity to testify today and look forward to an ongoing dialogue on this important subject. Epsilon supports national data breach notification legislation and stands ready to serve as a resource to this Committee as you continue to consider this critical issue.

About Epsilon

Epsilon is a leading provider of permission-based e-mail marketing services, and proudly claims as clients some of the world's largest and best-known consumer and financial service brands. The company's roots lie in the direct mail marketing industry, where for over 40 years Epsilon has provided valuable services to companies seeking to market to consumers directly

through means such as catalog marketing. Today, in addition to those and other related services, Epsilon also provides many well known companies and brands with a comprehensive e-mail marketing platform. Consumers choose (“opt-in”) to receive email communications from Epsilon’s clients. For example, consumers may choose to provide their e-mail addresses to an Epsilon client in order to receive discounts or other special offers. Epsilon provides the mechanism through which its clients can help ensure that consumer e-mail lists are maintained and messages to them are compliant with the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (“CAN-SPAM”), including managing consumer opt-out requests in the event that a consumer who has opted-in decides they no longer want to receive emails from the Epsilon client. Epsilon’s e-mail platform lets its clients – and Epsilon employees acting on their behalf as account managers – manage this data.

As a provider of data management services to major consumer brands and financial institutions, Epsilon is committed to responsible information governance and recognizes the importance of keeping client data secure. To enhance security across its infrastructure, Epsilon for the past several years has implemented and maintains an information security program conforming to data security standards set forth by the International Organization for Standardization (“ISO”). More specifically, Epsilon has implemented an ISO 27001¹ compliant information security management system that implements ISO 27002² controls. This system requires an information security program that assesses an organization’s information security risks, designs and implements comprehensive safeguards to control unacceptable risks, and

¹ International Organization for Standardization, ISO/IEC 27001:2005, http://www.iso.org/iso/catalogue_detail?csnumber=42103.

² International Organization for Standardization, ISO/IEC 27002:2005, http://www.iso.org/iso/catalogue_detail?csnumber=50297.

maintains that program to ensure continued improvement and ongoing assessments. The goal of the ISO 27002 standard is to facilitate best practices for controlling the types of information security risks to which companies like Epsilon might be exposed. Combined, the ISO 27001 standard and 27002 controls provide a process for comprehensive information security that is detailed, rigorous, and adaptable to changing circumstances.³

Epsilon was the first in its industry to become ISO 27001 certified. Epsilon has been ISO 27001 certified since 2006, and has subsequently received yearly re-certifications. Acquiring this certification is a thorough and demanding process. The certification process, which started in 2005, took nearly a year to complete and required validation from independent third-party auditors. Epsilon has maintained its ISO 27001 certification every year since then, undergoing yearly reviews that demand continual improvements to the company's information security program. By obtaining and maintaining this certification, Epsilon has demonstrated its commitment to ensuring that its information security program provides reasonable and appropriate safeguards for client and consumer data.

Incident Chronology

Like many other organizations, Epsilon's information security program is designed to identify and respond to attacks and threats. In identifying the recent attack on Epsilon's systems, the company's security program detected unauthorized download activity and invoked Epsilon's security incident response program. This led to an immediate move to investigate and remediate the unauthorized entry and to put in place additional safeguards based on the company's findings. The following is a brief chronology of the incident.

³ Ted Humphreys, *State-of-the-Art Information Security Management Systems with ISO/IEC 27001:2005*, ISO INSIDER, Jan.-Feb., 2006, available at http://www.iso.org/iso/info_security.pdf.

On March 30, an Epsilon employee contacted the e-mail application support team and reported unusual download activity that seemed suspicious. The Epsilon security investigation team responded immediately, beginning an internal investigation and reaching out to federal law enforcement authorities. Epsilon's internal investigation revealed that the login credentials of the employee had been compromised. As soon as Epsilon's investigators identified the compromised credentials, the security team disabled the credentials and began a forensic investigation of the relevant computer resources. Epsilon's immediate response activities included:

- Initiating additional virus scans of relevant systems.
- Revoking and re-issuing Epsilon system-user credentials for administrator-level users.
- Committing additional resources to monitoring unusual or suspicious activity.
- Beginning a forensic investigation to identify root causes.
- Notifying law enforcement including the FBI and Secret Service to seek their assistance, which resulted in the Secret Service beginning its investigation on April 1.

In addition to efforts to identify and contain the incident within the company, Epsilon also promptly began to assist its clients. These actions included:

- Contacting potentially affected clients and cooperating with them on an ongoing basis.
- Communicating with Epsilon's anti-virus support vendor to identify threat signatures and obtain additional support.

Epsilon has also worked to help address the concerns of consumers by providing public notice of the incident on the Epsilon website on April 1⁴ with an additional update on April 6⁵, and has set up an incident response center to answer questions from consumers and our corporate clients. Additionally, Epsilon has added information to its website to provide consumers with educational materials on guarding against phishing attacks.⁶ Specifically, this information explains what phishing attacks are, how they occur, and the steps a consumer can take to avoid becoming a victim.

On April 2, Epsilon met with its outside forensic consultants to review the evidence collected to date and confirm that information was flowing appropriately to the Secret Service. Epsilon's outside forensic consultants also reviewed the company's containment measures implemented thus far and, as the investigation unfolds, will make recommendations regarding further measures.

To date, the investigation has confirmed that only e-mail addresses and, in some cases, first and last names of consumers have been affected. At this time Epsilon has no evidence that any other data the company maintains were compromised in this attack. It appears that the attacker was only able to steal data from Epsilon's e-mail services platform; other platforms, such as its hosted client databases, were not affected. Going forward, Epsilon will continue to adhere to and improve its security policies and procedures, especially in light of this criminal

⁴ Press Release, Epsilon, Epsilon Notifies Clients of Unauthorized Entry into Email System (Apr. 1, 2011), http://www.epsilon.com/News%20&%20Events/Press_Releases_2011/Epsilon_Notifies_Clients_of_Unauthorized_Entry_into_Email_System/p1057-13.

⁵ Press Release, Epsilon, Alliance Data Provides Statement Surrounding Unauthorized Entry Incident at Epsilon Subsidiary (Apr. 6, 2011), http://www.epsilon.com/News%20&%20Events/Press_Releases_2011/Alliance_Data_Provides_Statement_Surrounding_Unauthorized_Entry_Incident_at_Epsilon_Subsidiary/p1061-13.

⁶ Epsilon, Consumer Information on Phishing, http://www.epsilon.com/Privacy%20Policy/Consumer_Information_on_Phishing/p467-12.

attack on its e-mail services platform. Further, Epsilon has engaged third-party experts to review and recommend additional hardening processes to the company's existing controls.

Data Breach Legislation

As the company's General Counsel, it is my job to make sure that we continue to work with law enforcement to make sure that we uncover all of the facts of this attack and to continue to improve security measures at the company every day. I am committed to doing so but also believe that Congress has an important role to play in protecting end consumers.

In this regard, Epsilon appreciates the opportunity to also provide input on potential data breach legislation being considered by the Subcommittee. Epsilon fully supports national legislation that would create a uniform standard for data breach notification. The current patchwork of individual state breach notification laws only serves to create confusion among consumers and businesses, and imposes unnecessary compliance costs. A uniform national law, on the other hand, would provide predictability and equity for consumers, regardless of their state of residence, and would make it much easier and less costly for business to ensure any applicable notification requirements are met.

Conclusion

For decades, Epsilon's commitment to trust and data security has helped the company build client relationships with some of the largest consumer and financial services brands in the world. Epsilon knows its clients, in turn, work hard to protect the privacy of consumers. For these reasons, Epsilon deeply regrets that the criminal activities of others have called into question this commitment. Epsilon is determined to investigate the unauthorized intrusion into the company's e-mail services platform thoroughly and remediate promptly and appropriately. As data management services become more sophisticated, criminals likewise are enhancing their

efforts to infiltrate even the most sophisticated systems. Epsilon will continue to respond to these criminal threats – by improving its own systems and working with law enforcement to try and apprehend those responsible for this intrusion. Our ultimate goal is to ensure reasonable protections for data management, our clients, and, most importantly, the end consumers.

I sincerely hope that the information I am able to provide at this hearing is helpful to the Subcommittee. Epsilon looks forward to working with the Subcommittee to help it understand the data security challenges that companies are continually facing, and to provide input on effective data security legislation that is in the best interests of both consumers and businesses.

Thank you.