FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

April 6, 2011

Mr. Ed Heffernan
President and Chief Executive Officer
Alliance Data Systems, Inc.
7500 Dallas Parkway, Suite 700
Plano, TX 75024

Dear Mr. Heffernan:

We write today regarding the recent data breach experienced by the marketing firm Epsilon that falls under the umbrella of Alliance Data Systems, Inc. According to recent press reports, the Epsilon breach that occurred within the last week impacted costumers of some of the largest banks and retail companies in the United States. JPMorgan Chase, Best Buy, Home Shopping Network, Walgreens, Kroger, Verizon, Barclays Bank of Delaware, and Capitol One are among Epsilon's customers identified in those reports.

Those reports also describe this breach event as only relating to the release of customer email addresses and names; however, in this day and age, even this information can lead to an unfortunate attack on an individual's identity – especially if the consumer's information is paired with the correct retailer or bank. In the simplest fashion, a criminal can easily create a phishing email that could lead an unwitting consumer into financial disaster. With a reported 40 billion marketing emails sent a year, the Epsilon breach could potentially impact a historic number of consumers.

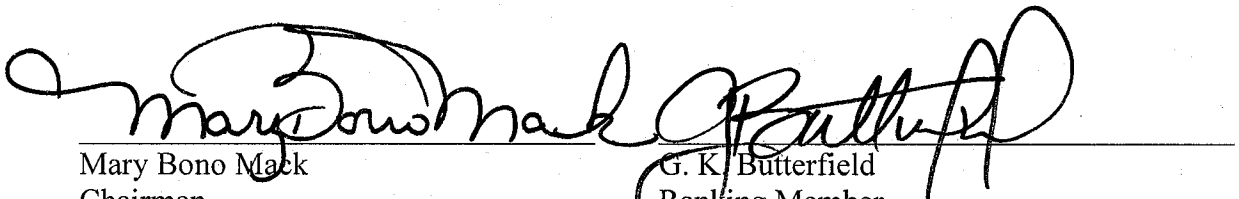
The Subcommittee on Commerce, Manufacturing and Trade has a longstanding history of interest in consumer privacy, in addressing identity theft, and in industry efforts to address the threats posed by data breach. Events such as this one directly inform our efforts in the data security arena. As a result, we request an answer to the following questions no later than April 18, 2011.

1. When did you, including your online marketing arm, Epsilon, become aware of the data breach?
2. How did you become aware of the breach?
3. When did you notify the appropriate authorities of the breach?

4. When did you notify your corporate customers of the breach?
5. When did you notify the consumers whose data was breached?
6. How many consumers were impacted by this breach, and how did you ascertain the number?
7. How many companies were impacted in the data breach? Please identify the companies involved in this event.
8. Have you identified how the breach occurred?
9. Have you identified the individual(s) responsible for the breach?
10. What information was obtained by the unauthorized individual(s) a result of this breach, and how did you ascertain this information?
11. What steps have you taken or do you plan to take to prevent future such breaches?
12. Do you currently have a privacy policy that addresses data retention practices? If not, why not? If so, what are those practices and do you plan any changes in your policies as a result of this breach?
13. Regarding the information obtained in the breach, how long had that personal data been retained?
14. What steps have you taken or do you plan to take to mitigate the effects of this breach? Do you plan to offer any credit monitoring or other services to consumers who suffer actual harm as a result of this breach?

Thank you for your attention to and assistance in this matter.

Sincerely,



Mary Bono Mack
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

G. K. Butterfield
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade

cc: The Honorable Fred Upton, Chairman

The Honorable Henry A. Waxman, Ranking Member