SIDLEY AUSTIN LLP
SIDLEY

SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
(202) 736 8000
(202) 736 8711 FAX

emcnicholas@sidley.com
(202) 736 8010

BEIJING
BRUSSELS
CHICAGO
DALLAS
FRANKFURT
GENEVA
HONG KONG
HOUSTON
LONDON

LOS ANGELES
NEW YORK
PALO ALTO
SAN FRANCISCO
SHANGHAI
SINGAPORE
SYDNEY
TOKYO
WASHINGTON, D.C.

FOUNDED 1866

April 26, 2013

**By FedEx**

Attorney General Michael A. Delaney
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: LivingSocial Security Incident

Dear Attorney General Delaney:

We write to advise the Commission's staff of an information security incident involving an unauthorized intrusion into sensitive information systems at our client, LivingSocial, Inc. ("LivingSocial").

On or about April 12, 2013, LivingSocial first became aware that the security of some of its systems may have been compromised beginning approximately April 5, 2013, although the investigation into the incident is continuing. Based on current information, we understand that the intruder(s) used compromised credentials to gain information about elements of LivingSocial's production environment and to extract certain information from its servers. In particular, LivingSocial's current understanding is that the intruders gained access to information including names, email addresses, date of birth for some users, and "hashed" and "salted" passwords if the user had entered a password. In total, we currently believe that information for at least 29 million Americans was compromised, as well as several million individuals in other countries. The number of affected individuals in any given State remains uncertain. LivingSocial is working on methods to develop reliable estimates, but those estimates are not available at this time.

Based upon our current understanding of the incident, we believe that the risk of harm to consumers is low, given the nature of the information accessed. Importantly, we have no evidence that there was unauthorized access to the separate systems that store LivingSocial's customers' credit cards. In addition, LivingSocial's merchant's financial and banking information was not affected or accessed by this incident.

Regarding the passwords at issue, although they were hashed and salted, given time, it would conceivably be possible for the intruder to reverse-engineer them. To mitigate this risk, LivingSocial has forced a reset of all consumer passwords. In addition, LivingSocial is sending email notice to LivingSocial customers who had entered passwords, customers who used Facebook connect, and users without passwords. LivingSocial has also posted extensive FAQs with information regarding identity theft and fraud protection. We are hopeful that, given the narrow scope of the information extracted and the company's mitigation measures, these steps will effectively eliminate the risk of harm to LivingSocials' customers.

With the support of GuidePoint Security and Navigant, LivingSocial is continuing to actively review this incident and its processes, including its processes for ensuring its continuing compliance with the US-EU Safe Harbor as well as PCI-DSS requirements. LivingSocial is committed to increasing the security of its systems in order to prevent the recurrence of such an incident and to protecting the privacy and security of its customers. For instance, two-factor authentication has been mandated for VPN access in order to minimize user account compromise. In addition, LivingSocial has reconfigured the relevant firewall rules to blacklist the active hosts and has elevated its monitoring for malicious IP addresses, VPN, and privileged account use.

This information is being provided to various relevant regulators as contemporaneously as is feasible, including various state attorneys general and the United Kingdom's Information Commissioner's Office. LivingSocial would be pleased to work with law enforcement and regulators to bring the hackers responsible for this intrusion to justice, and to provide more detailed briefings, as is appropriate to the circumstances, about the scope, signature, and effects of the attack to interested regulators and other stakeholders.

If you have any questions about this incident, please do not hesitate to contact me at the number listed above.

Sincerely,

Edward R. McNicholas

Edward R. McNicholas