LPL Financial

Keith H. Fine
Senior Vice President
Associate Counsel

One Beacon Street, 22nd Floor
Boston, MA 02108-3106
keith.fine@lpl.com
617 897 4425 *office*
800 775 4575 *ext.* 4425
617 426 8589 *fax*

May 6, 2008

Attorney General Kelly A. Ayotte
New Hampshire State Attorney General's Office
33 Capitol Street
Concord, NH 03301

Re: LPL Financial Corporation
Notification of Potential Security Breach under N.H. Rev. Stat. § 359-C:20
Vehicle Break-In: Laptop Stolen

Dear Attorney General Ayotte:

We write to advise you of an incident involving a burglary of a vehicle belonging to an LPL Financial ("LPL") employee, which resulted in a stolen laptop containing personal data of residents of New Hampshire. The incident occurred in East Stanley, North Carolina on April 10, 2008. To our knowledge, the laptop contained certain personal information of about 2,800 employees of LPL and its affiliated companies, only three of whom are New Hampshire residents.

Learning About the Incident. On April 10, 2008 one or more unknown persons stole a laptop computer from the vehicle of an LPL employee. The laptop contained names, Social Security numbers, employee ID and other employment and compensation information of LPL employees. The laptop did not contain any home addresses. A list containing the names and addresses of affected New Hampshire residents are attached to this letter as Exhibit A.

LPL first learned of this incident on April 10, 2008 and took the following actions: (1) notified law enforcement; (2) investigated the situation; (3) determined what information had been compromised; and (4) will notify and offer solutions to the affected individuals.

At this time, LPL has no specific knowledge that any employee information was accessed or misused as a consequence of the breach. We also are unaware of any reported instance of identify theft related to this incident.

Investigating the Disclosure. As noted above, we determined that the stolen laptop contained certain personal information of three New Hampshire residents. Internal reports were run to identify all of the individuals whose information could have been accessed on the laptop. These internal reports were then used to generate mailing lists for the employee notifications discussed below.

Communicating with Affected Individuals. In order to ensure that affected individuals could take immediate steps to protect themselves from possible identity theft or other monetary damage, LPL will promptly notify them of the incident by sending notices via first-class mail by May 9, 2008. The notification materials, attached to this letter as Exhibit B, will advise employees to remain vigilant by reviewing account statements and monitoring free credit reports.

Services to Affected Individuals. The notification materials will also describe the various services LPL has made available to affected individuals through Kroll, Inc. ("Kroll"), a risk consulting company. LPL has instructed Kroll to provide affected individuals toll-free access to its Consumer Solutions Center, along with credit monitoring services and identity theft restoration services. Kroll will also provide access to a credit report to affected individuals who enroll for the service. In addition, the enrolled individual's credit file will be monitored for critical changes, including address changes, inquiries, new trade-lines, derogatory notices and appearance of certain public records. Individuals will be informed of such changes by either postal or electronic mail. If a person suspects or discovers fraudulent activity, Kroll, as part of the identity restoration services, will provide the affected individual with a toolkit of resources to address issues encountered.

LPL believes the services offered to its employees will help them immediately respond to any threats of identity theft or other misuse of their data as a result of this isolated incident.

Efforts to Deter Future Breach. LPL has taken several important steps to improve the level of its data security by increasing the profile of data security issues within the company at all levels, up to and including senior management. In March 2008, LPL hired Marc Loewenthal as SVP – Chief Security/Privacy Officer, a newly created position at LPL. Mr. Loewenthal has extensive experience in the area of data protection. As a member of senior management, he reports directly to the Chief Risk Officer of LPL.

In addition, LPL has developed a new, comprehensive information privacy and security program, with new policies and procedures that were implemented in April 2008. LPL has also begun a project to encrypt data maintained on the laptops used by its employees and representatives.

We trust that this letter and its enclosures provide you with all the information required to assess this incident and LPL's response. Please let us know if you have additional questions or if we can be of further assistance.

Sincerely,

Keith H. Fine

Enclosures

cc: Marc Loewenthal
Edwards Angell Palmer & Dodge LLP
Theodore P. Augustinos
Mark E. Schreiber

Exhibit B

Urgent Message
Please Open Immediately.

[Name]
[Address]

Dear [Employee Name]

Guarding the privacy of our valued employees is a top priority at LPL Financial and its affiliated companies. We maintain a strong commitment to protecting your information and aim to communicate openly should it ever be compromised. Regrettably, a laptop containing personal information was stolen from one of our employees on April 10, 2008. This information included your name, Social Security number, employee ID and other employment and compensation information. Your home address and date of birth were not included in this database.

While we have no evidence that the information has been misused, we wanted to make you aware of the incident and the steps we are taking to help safeguard your personal information. First, we are beginning the process of encrypting all laptops in order to enhance their security and prevent a reoccurrence of this type of incident. Second, we have published guidelines on the proper use of laptops and what is expected of employees that use laptops to protect the confidentiality of sensitive information.

We have also engaged Kroll, Inc. to provide its ID TheftSmart service; in fact, this packet was mailed from Kroll's print facility in Georgia to expedite delivery. Kroll's service, offered at no cost to you, includes access to Enhanced Identity Theft Restoration, Continuous Credit Monitoring, and a Trimerged Credit Report.

ID TheftSmart is one of the most comprehensive programs available to help protect your name and credit against identity theft. We encourage you to take the time to review the safeguards made available to you and review your statements and credit information regularly.

If you have any questions or feel you have an identity theft issue, please call ID TheftSmart at 1-800-588-9839 between 8:00 a.m. and 5:00 p.m. (Central Time), Monday through Friday. If you want to talk to someone at LPL Financial to clarify or discuss the authenticity of this letter, please contact Keith Fine at 617-423-3644, ext. 4425, or Marc Loewenthal at 858-450-9606, ext. 7214.

We apologize for any inconvenience or concern this situation may cause. We at LPL Financial believe it is important for you to be fully informed of any potential risk resulting from this incident. Again, we want to reassure you that we have no evidence that your personal information has been misused. We remain committed to maintaining

privacy of your information as a key priority and will continue to take the needed steps to protect your information.

Sincerely,

Esther Stearns
President
LPL Financial

Enclosures:
Membership Card
A Summary of Your Rights Under the Fair Credit Reporting Act
Authorization Form for Credit Report and Credit Monitoring Service
Service Overview Brochure
Kroll Privacy Policy