

May 6, 2008

Attorney General Douglas F. Gansler  
Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202

**Re: LPL Financial Corporation  
Notification of Potential Security Breach under Md. Code, Com Law § 14-3504  
Log-On Passwords Compromised**

Dear Attorney General Gansler:

We write to advise you of incidents in which hackers compromised the logon passwords of fourteen financial advisors and four assistants of LPL Financial (“LPL”). To our knowledge, the hackers used these passwords to gain access to customer accounts in order to “pump and dump” penny stocks. These incidents affected approximately 10,219 individuals, of whom only 19 are Maryland residents.

At this time, LPL has no specific knowledge that any customer information was accessed or misused as a consequence of the breach described above. We also are unaware of any reported instance of identify theft related to these incidents. As described below, LPL learned of the first incident on July 16, 2007 and took the following actions: (1) notified law enforcement; (2) notified our primary regulator, the Financial Industry Regulatory Authority; (3) investigated the situation; (4) determined what information had been compromised; and (5) notified and offered solutions to the affected individuals.

Further information concerning these incidents and LPL’s response is provided below. LPL plans to send a supplemental notice to these residents in order to satisfy the specific disclosure requirements of the Maryland statute. Please note that since the time of the incident and the mailing of the original notices, LPL has taken several important steps to improve its level of data security and compliance with Maryland requirements for responding to breaches. LPL has increased 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. In August 2007, LPL engaged the services of Kroll Inc. ("Kroll"), a risk consulting company, to provide various services as further described below and in LPL's customer notice, a copy of which is enclosed. In addition, LPL has commenced a project to enhance security on its advisor facing trading and operations systems in September 2007 and expects the project to complete in December 2008. LPL has also developed a new, comprehensive information privacy and security program, with new policies and procedures that will be implemented this month. Finally, LPL recently engaged the services of Edwards Angell Palmer & Dodge LLP to advise Mr. Loewenthal and LPL's in-house counsel as needed on information privacy and security issues.

**Learning About the Incidents.** Hackers compromised the logon passwords of fourteen financial advisors and four assistants in branch offices located in New Jersey, Illinois, Rhode Island, Pennsylvania, Colorado, Texas, California, Georgia and Connecticut over the course of several months. LPL learned of the first incident on July 16, 2007. The information that was potentially accessible included unencrypted names, addresses and Social Security numbers of customers and non-customer beneficiaries. LPL cannot determine whether this information was actually accessed.

**Investigating the Disclosure.** As noted above, LPL determined that the logon passwords were used to gain access to customer accounts, including the accounts of 19 Maryland individuals. The passwords were used to gain access to consumer accounts in order to "pump and dump" penny stocks. Attempted transactions were intercepted and either rejected or reversed. No losses were passed on to the customers.

**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 moved quickly to inform them of the incident. LPL instructed Kroll to provide toll-free access to its Consumer Solutions Center, along with credit monitoring services and identity theft restoration services. With the assistance of Kroll, LPL prepared guidance for call center representatives and drafted a communication to affected individuals. The communication was sent by first-class mail on the following dates: 9/21/07; 9/26/07; 10/12/07; 12/11/07; 12/17/07; 2/26/08; 3/7/08; 3/14/08; and 3/17/08. At the advice of Kroll, notices to affected individuals included the information on the attached letter. A copy of the form of the original notification materials provided to the affected Maryland residents is enclosed as Exhibit A.

The notification materials also advised consumers to remain vigilant by reviewing account statements and monitoring free credit reports. During the time between learning of the incident in July 2007 and sending notices to affected customers on the dates listed above, LPL diligently investigated the breach. The investigation process took several months to complete as, among other things, LPL had to discern the specific type of information accessed and the individuals affected.

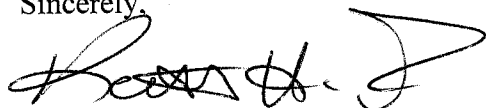
Based on the advice of outside counsel, LPL intends to send a supplemental notice by May 9, 2008 to the affected individuals with additional information now required under the Maryland law. The form of this supplemental notice is provided as Exhibit B to this letter.

**Services to Affected Individuals.** As noted above, LPL also took proactive steps to help individuals protect themselves against identity theft by purchasing credit monitoring and identity restoration services from Kroll for affected individuals, and referenced this also in the original notice, the form of which is enclosed as Exhibit A. Kroll will 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. As noted above, at this time, LPL has no specific knowledge that any customer information was accessed or misused as a consequence of the breach described above, and is unaware of any reported instance of identify theft related to this incident.

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

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



Care of: ID TheftSmart 600 Satellite Blvd | Suwanee, GA 30024

Urgent Message.  
Please Open Immediately.

<FirstName> <MiddleInitial> <LastName>  
<Address> (Line 1)  
<Address> (Line 2)  
<City> <State> <Zip>  
<POSTNET BARCODE>

<As a valued Customer of John Doe Financial Advisor>

Dear <FirstName> <MiddleInitial> <LastName>,

We are writing to notify you of a recent event that could affect you as a customer of LPL Financial. Recently, we learned an unauthorized person(s) obtained access to the system your financial advisor uses for trading and operation at LPL Financial. The potentially accessible information through this system could include names, addresses, phone numbers, account numbers, Social Security numbers, and dates of birth.

While we have no indication that your information has been misused, we wanted to make you aware of the incident and the steps we are taking to prevent a reoccurrence. We are currently conducting a comprehensive review of this matter to determine how the unauthorized access occurred, and have taken immediate measures to further secure our systems to the greatest extent possible.

As part of enhancing our security measures, you have the opportunity to request a new LPL Financial account number. To begin the process, please contact your financial advisor.

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 read about the safeguards now available to you.

If you have any questions or feel you have an identity theft issue, please call ID TheftSmart at 1-800-588-9839 between 9:00 a.m. and 6:00 p.m. (Eastern Time), Monday through Friday. If you want to talk to someone at LPL Financial to clarify or discuss the contents of this letter, please call us 800-558-7567, option 3 – Customer Service, between 9:00 a.m. and 6:00 p.m. (Eastern Time), Monday through Friday.

We appreciate the trust placed in LPL Financial and deeply regret any inconvenience this incident may have caused you. We remain committed to customer privacy being a key priority and will continue to take the needed steps to protect your information.

Sincerely,

Steven M. Black  
Chief Risk Officer  
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

974330LKRO-0108

Member FINRA/SIPC



<FirstName> <MiddleInitial> <LastName>  
Membership Number: <Membership Number>

Member Services: 1-800-588-9839  
9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday  
If you have questions or feel you may have an identity theft  
issue, please call ID TheftSmart member services



<FirstName> <MiddleInitial> <LastName>  
Membership Number: <Membership Number>

Member Services: 1-800-588-9839  
9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday  
If you have questions or feel you may have an identity theft  
issue, please call ID TheftSmart member services

Please detach cards and keep in a convenient place for your reference

[Date]

[Name]

[Address]

Dear <FirstName> <MiddleInitial> <LastName>,

On **[date]**, we may have notified you regarding an incident in which your personal information, including your name, address and social security number, maintained on our trading and operation database may have been accessed. This letter supplements our previous notice concerning that incident with additional information.

While we have no indication that your information has been misused, we wanted to make you aware of the incident and the steps we are taking to prevent a reoccurrence. We are currently conducting a comprehensive review of this matter to determine how the unauthorized access occurred, and have taken immediate measures to further secure our systems to the greatest extent possible.

As we indicated in our letter of **[date]**, we have also engaged Kroll Inc. to provide its ID TheftSmart™ service. 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. Your membership card and a package of information regarding identity theft solutions were enclosed with the letter sent on **[date]**. We encourage you to read about the safeguards available to you.

If you have any questions or feel you have an identity theft issue, please call ID TheftSmart at 1-800-588-9839 between 9:00 a.m. and 6:00 p.m. (Eastern Time), Monday through Friday. If you want to talk to someone at LPL Financial to clarify or discuss the contents of this letter, please call us 1-800-558-7567, option 3 – Customer Service, between 9:00 a.m. and 6:00 p.m. (Eastern Time), Monday through Friday.

In addition to ID TheftSmart, you may also obtain information regarding steps you can take to avoid identity theft from the following sources:

- Equifax Credit Information Services, Inc.  
P.O. Box 740241  
Atlanta, GA 30374  
1-888-766-0008
- TransUnion Fraud Victim Assistance Department  
P.O. Box 6790  
Fullerton, CA 92834  
1-800-680-7289

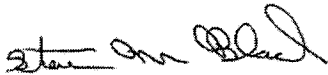
Experian  
475 Anton Blvd.  
Costa Mesa, CA 92626  
1 714 830 7000  
1-888-397-3742

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-FTC-HELP (1-877-382-4357)  
<http://www.ftc.gov>

Maryland Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
<http://www.oag.state.md.us/index.htm>

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

Sincerely,



Steven M. Black  
Chief Risk Officer  
LPL Financial