

# BakerHostetler

## Baker&Hostetler LLP

811 Main Street  
Suite 1100  
Houston, TX 77002-6111

T 713.751.1600  
F 713.751.1717  
www.bakerlaw.com

William R. Daugherty  
direct dial: 713.646.1321  
wdaugherty@bakerlaw.com

November 16, 2018

### **Via Email (securitybreach@atg.wa.gov) and Overnight Mail**

Office of the Washington Attorney General  
Consumer Protection Division  
800 5th Ave, Suite 2000  
Seattle, WA 98104-3188

*Re: Incident Notification*

Dear Sir or Madam:

On behalf of our client, LPL Financial LLC (LPL), we are writing to notify you of a data security incident that occurred at an LPL third-party service provider, Capital Forensics, Inc. (CFI).

CFI is a firm that provides consulting and data analysis to assist firms with regulatory, compliance, and risk management activities. On November 1, 2018, LPL was notified by CFI that, on the same day, an unauthorized person appears to have accessed a single CFI user's account at a third party file-sharing system that CFI uses to share data with its customers, including LPL. CFI reported that it promptly secured the CFI user's account the same day but that files containing LPL client information were among the data potentially accessed. Upon learning this, LPL immediately launched an investigation and coordinated with CFI to ensure that the LPL data, including client information, was removed from that file-sharing system. Working with CFI, LPL conducted a thorough review of the files and determined that the files included some of LPL's clients' personal information, which varied by individual but could have included the client's name, LPL account number, and Social Security number.

Beginning on November 17, 2018, LPL will start mailing notification letters to 8,127 Washington residents in accordance with Wash. Rev. Code § 19.255.010 in substantially the same form as the attached letter. LPL has provided a telephone number that individuals can call with questions. LPL has also arranged for individuals to receive two years of complimentary credit monitoring and identity protection services from AllClear ID.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Office of the Washington Attorney General

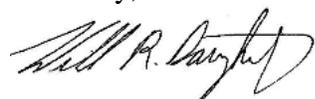
November 16, 2018

Page 2

Protecting investor information is a top priority for LPL, and LPL has implemented heightened monitoring on the LPL accounts involved. Law enforcement has also been notified of the incident.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "William R. Daugherty". The signature is fluid and cursive, with the first name "William" being the most prominent.

William R. Daugherty

Partner

Enclosure

19413  
K831916

November 17, 2018

Dear [REDACTED],

LPL Financial LLC works with your financial advisor and is the broker-dealer and custodian for your accounts. In this role, protecting the privacy of your personal information is a top priority. Regrettably, we are writing to inform you of a data security incident that has occurred at one of our service providers, Capital Forensics, Inc., that may have involved some of that information. This notice describes the incident, the measures we have taken, and some steps you can take in response, including taking advantage of credit monitoring and identity protection services at no charge to you.

Capital Forensics is a firm that provides consulting and data analysis to assist firms with regulatory, compliance, and risk management activities. On November 1, 2018, Capital Forensics notified LPL that, on the same day, an unauthorized person appears to have gained access to a single Capital Forensics user's account on a third party file-sharing system it uses to share data with customers, including LPL. Capital Forensics reported that it promptly secured the Capital Forensics user's account that same day but that files containing LPL client information were among the data potentially accessed. Upon learning this, we immediately launched an investigation and coordinated with Capital Forensics to ensure that the LPL data, including client information, was removed from that file-sharing system. Working with Capital Forensics, we conducted a thorough review of the files and determined that the files included some of your personal information, including your account number and Social Security Number.

We want to make you aware of the incident and let you know that we are offering you a two-year membership in AllClear ID at no cost to you. This membership will include two separate services: identity protection and fraud alerts with credit monitoring. The services are available to you immediately and you can begin using them at any time during the next 24 months.

**AllClear Identity Repair: This service is automatically available to you with no advance enrollment required.** If a problem arises, simply call 1-855-683-1166 and a dedicated investigator will help recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.



AllClear Fraud Alerts with Credit Monitoring: **You will need to enroll in this service if you wish to take advantage of it.** This service offers the ability to place 90-day fraud alerts on your credit file to help protect you from credit fraud and then to remove or renew those alerts at any time. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. **To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) or by phone by calling 1-855-683-1166 using the following redemption code: [REDACTED].**

Please note: After you enroll, you will need to take some additional steps to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required to activate your monitoring options. Those will be communicated to you by AllClear ID when you enroll. **For more information on additional steps you can take to protect your personal information, please see the pages that follow this letter.**

We apologize for any inconvenience or concern this incident may cause. We have implemented heightened monitoring on the LPL accounts involved, including yours, and law enforcement has also been notified of the incident.

If you have questions, please call 1-855-683-1166, Monday through Saturday between the hours of 9:00 a.m. and 9:00 p.m. EST.

Sincerely,

A handwritten signature in black ink, appearing to read "Gerald F. Spada". The signature is fluid and cursive, with the first name "Gerald" and last name "Spada" clearly legible.

Gerald F. Spada  
Senior Vice President, Chief Privacy Officer

## **Additional Steps You Can Take**

Regardless of whether you choose to take advantage of this free credit monitoring, we encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on financial accounts, you should immediately contact your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800  
*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW  
Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**If you are a resident of Connecticut, Maryland, North Carolina, or Rhode Island**, you may contact and obtain information from your state attorney general at:

*Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318,  
[www.ct.gov/ag](http://www.ct.gov/ag)

*Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202,  
[www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023 (toll free when calling within Maryland)  
(410) 576-6300 (for calls originating outside Maryland)

*North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC  
27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716-6400

*Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903,  
[www.riag.ri.gov](http://www.riag.ri.gov), 1-401-274-4400

Note that pursuant to Rhode Island law, you have the right to file and obtain a copy of any police report.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the



appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)  
**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

**Fair Credit Reporting Act:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit [www.ftc.gov/credit](http://www.ftc.gov/credit). The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

