

BakerHostetler

Baker & Hostetler LLP

999 Third Avenue
Suite 3600
Seattle, WA 98104-4040

T 206.332.1380
F 206.624.7317
www.bakerlaw.com

Randal L. Gainer
direct dial: 206.332.1381
rgainer@bakerlaw.com

August 28, 2015

VIA OVERNIGHT DELIVERY

Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attn: Attorney General Joseph Foster

Re: Incident Notification

Dear Attorney General Foster:

Our client Viewpoint, Inc. dba Viewpoint Construction Software ("Viewpoint") is writing to inform you of an incident involving unauthorized changes to certain employee direct deposit routing information in its electronic payroll system.

On July 15, 2015, Viewpoint learned that, on July 9, 2015, an unauthorized person gained access to Viewpoint's electronic payroll system and modified the direct deposit routing instructions for 115 employee records. Viewpoint later determined through a forensic investigation that the unauthorized person had used malware to obtain a Viewpoint manager's user-name and password to gain access to the payroll system. While in the system, the perpetrator may have had access to certain personal information, including employee names, addresses, Social Security numbers, salaries, email addresses and direct deposit information.

When Viewpoint learned of this incident, it immediately took steps to identify and address the issue. Viewpoint also notified federal authorities and began working closely with Mandiant – a leading independent forensics firm – to investigate the incident, and corrected the direct deposit routing records to ensure that all employees received their payroll deposits.

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

STATE OF NH
DEPT OF JUSTICE
2015 AUG 31 AM 9:41

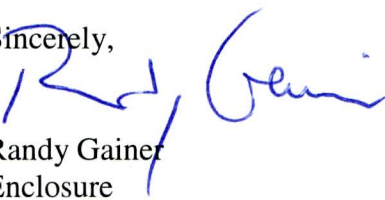
Attorney General Joseph Foster
August 28, 2015
Page 2

While the investigation was still ongoing, Viewpoint provided advanced notice to all employees on July 22, 2015 and provided complimentary one-year membership to Experian's® ProtectMyID® Alert. Now that the investigation is almost finished, Viewpoint will also be providing formal written notice, starting on August 28, 2015.

To help prevent something like this from happening in the future, Viewpoint has been working with an outside security firm to implement additional safeguards and will be conducting a comprehensive review of its information security practices and procedures.

Attached is a sample of the notification letter being sent to affected individuals. Viewpoint is notifying two New Hampshire residents of this incident. Please do not hesitate to contact me if you have any questions.

Sincerely,



Randy Gainer
Enclosure

VIEWPOINT

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>

<<Name>>

<<Address1>>

<<City>> <<State>> <<Zip>>

<<Date>>

Dear <<Name>>:

As a follow up to the email that we sent to all U.S. employees on July 22, 2015 regarding the incident that may have involved some of your personal information as an employee of Viewpoint, we wanted to provide you with an update.

What happened?

On July 15, 2015, Viewpoint learned that, on July 9, 2015, an unauthorized person gained access to Viewpoint's records in the Ultipro payroll system and modified the direct deposit routing instructions for 115 employee records. The unauthorized person may have also accessed employee records containing certain personal information, including employees' names, addresses, Social Security numbers, salaries, email addresses and direct deposit information. If you were impacted, you would have received a direct email from me on July 22, 2015 with a subject titled, "Impacted Employees of the Security Breach."

What actions did Viewpoint take?

We want to assure you that nothing is more important to us than protecting the privacy and security of your information, and we continue to take this incident very seriously. When we learned of the unauthorized access to the payroll system, we immediately took steps to identify and address the issue. We notified federal authorities and began working closely with Mandiant – a leading independent forensics firm – to investigate the incident, and corrected the direct deposit routing records to ensure that all employees received their payroll deposits.

What is Viewpoint doing to protect me?

In addition to correcting the unauthorized changes to payroll routing records, we have arranged for you to receive a one-year membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. This product is being offered to all U.S. employees regardless of whether your direct deposit routing instructions were affected by this incident.

For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the "Activate ProtectMyID Now in Three Easy Steps" document enclosed with this letter. Also, please review the enclosed "Information about Identity Theft Protection" reference guide on the back of this letter, which describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

What is Viewpoint doing to prevent this from happening in the future?

We deeply regret any inconvenience this incident may cause you and are taking additional actions to enhance our IT systems moving forward to help prevent against similar incidents in the future.

If you have any questions, please call 1-888-643-2170, Monday through Friday from 7:00 AM to 7:00 PM Pacific Standard Time.

Sincerely,



Jennifer E. Yruegas, General Counsel

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
800-685-1111
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19022
800-888-4213
www.transunion.com

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that 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 at the toll-free numbers listed below:

Equifax
877-478-7625

Experian
888-397-3742

TransUnion
800-680-7289

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Activate ProtectMyID Now in Three Easy Steps

1. **ENSURE That You Enroll By: October 31, 2015** (Your code will not work after this date.)
2. **VISIT the ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. **ROVIDE Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **PC95573**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

**Activate your membership today at www.protectmyid.com/redeem
or call 877-288-8056 to register with the activation code above.**

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8056.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.