

[Paul Stuart Letterhead]

June \_\_, 2016

[Employee Name]

[Employee Address]

Re: Notice of Data Breach

Dear [Employee],

Paul Stuart greatly values the relationship we have with our employees and understands the importance of protecting the personal information you provide us. Regrettably, we are writing to inform you of an incident that involved some of your information. We are bringing this incident to your attention so that you can be alert to signs of any possible misuse of the information. This letter also describes credit protection services we are providing to you free of charge and other steps you can take to protect yourself.<sup>1</sup>

### **What Happened**

On Tuesday, May 10, a Paul Stuart employee mistakenly responded to a phishing email by releasing confidential personally identifiable employee information. We identified the incident on June 14, and immediately proceeded to take appropriate corrective measures. No customer information was involved.

This incident appears to be part of an increasingly common tax fraud scheme in which company employees are sent emails purporting to be from company executives that request personal information on employees, which can then be used to file fraudulent tax returns on behalf of employees. See <https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s>.

We are actively investigating the matter and the extent of the inappropriate data release. We have identified the cause of the release and are taking mitigating actions. We view the perpetrator's actions as criminal conduct and will be cooperating with law enforcement in this matter. We have already notified the FBI of this incident.

### **What Information Was Involved**

The employee information disclosed included name, Social Security number, home address, and salary. At this time, we have found no other evidence that your personal information has been

---

<sup>1</sup> This notification was not delayed as a result of a law enforcement investigation.

misused. Nevertheless, misuse of your information is possible given the intentional nature of the breach and the type of personal information that was obtained.

## **What We Are Doing**

In response to this incident, we are strengthening our defenses against phishing attacks, including new measures that will identify incoming external emails with higher risk of being fraudulent. We are also strengthening our cyber security training, including training with respect to phishing attacks, as part of a general training program that will be implementing next week.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

**AllClear SECURE:** The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

**AllClear PRO:** This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](https://enroll.allclearid.com) using the following redemption code: **{RedemptionCode}**.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

## **What You Can Do**

Regardless of whether you take advantage of the identity theft protection and credit monitoring services that we are offering, we encourage you to take these additional measures to monitor and protect against unauthorized use of your personal information:

- Regularly monitor your financial accounts and, if you see any unfamiliar activity, contact your financial institution.
- Obtain a free credit report from each of the three national consumer credit reporting companies (Equifax, Experian, and TransUnion) by calling (877) 322-8228 or by logging onto [www.annualcreditreport.com](https://www.annualcreditreport.com).
- Contact the three national consumer credit reporting companies for information about placing a “fraud alert” and/or a “security freeze” on your credit report to further detect any possible misuse of your personal information.

Equifax

Experian

TransUnion

P.O. Box 105069  
Atlanta, GA 30348  
(800) 685-5000  
[www.equifax.com](http://www.equifax.com)

P.O. Box 4500  
Allen, TX 75013  
(888) 397-3742  
[www.experian.com](http://www.experian.com)

(877) 322-8228  
P.O. Box 105281  
Atlanta, GA 30348  
[www.transunion.com](http://www.transunion.com)

- Because Social Security numbers were disclosed in this breach, there is the potential for tax-related identity theft, which occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund. Complete and submit the attached Form 14039 Identity Theft Affidavit to the IRS. In completing the Form 14039, you should check the box in Item 2. The description of the event that must accompany Item 2 may be taken from the first two paragraphs of this letter under the heading “What Happened.” For more information on tax-related identity theft see <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>.
- If you have not already filed your most recent tax return, consider filing your tax return electronically at the earliest convenience. If your electronic return has already been filed, that may dissuade perpetrators from attempting to file a fraudulent return in your name.
- Contact the Federal Trade Commission for additional information about “fraud alerts” and “security freezes,” and about how to monitor and protect your credit and finances. We encourage you to read the materials on the FTC website regarding preventing fraud and identity theft in order to better understand how criminals may seek to obtain your personal information. For example, one common scam involves phone calls or emails from thieves who pretend to be from the IRS (*see* <https://www.irs.gov/uac/stay-vigilant-against-bogus-irs-phone-calls-and-emails>).

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, D.C. 20580  
(202) 326-2222  
[www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-identity-theft)

- Maryland residents can contact the Maryland Office of the Attorney General for additional information about how to monitor and protect your credit and finances.

Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
(410) 576-6300  
1 (888) 743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

## **For More Information**

We understand that this incident may pose an inconvenience to you, and we sincerely apologize and regret that this situation has occurred. Paul Stuart is committed to protecting the privacy and

security of our employees' information, and we want to assure you that we have implemented appropriate policies and procedures to safeguard that information. Unfortunately, it is difficult to *fully* defend against criminal attacks and thefts.

If you have any questions regarding this incident or if you desire further information or assistance, please call [\_\_\_\_\_] at (\_\_\_\_) \_\_\_\_-\_\_\_\_.

Please respect the sensitivity of this matter and do not discuss it or share this letter or other related communications with anyone outside Paul Stuart, except as necessary for you to protect yourself against potential fraud or identity theft.

Sincerely,

Paulette Garafalo  
Chief Executive Officer