BASS BERRY + SIMS PLC

150 Third Avenue South, Suite 2800
Nashville, TN 37201
(615) 742-6250

March 7, 2016

U.S. Certified Mail

Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. Ann. §§ 359-C:1, we are writing on behalf of our client, Applied Systems, Inc. ("Applied"), to notify you of an unauthorized access or use of personal information affecting a New Hampshire resident.

Synopsis of the Incident Resulting in Unauthorized Access to Personal Information

Applied provides insurance software solutions and services to insurance agencies, brokerages and insurers. Recently, Applied discovered that one of its employees having responsibilities over payroll information was targeted by an email "phishing" scheme. On February 19, 2016, in response to what appeared to the employee to be a legitimate request for such information from Applied's CFO, the employee sent outside the company two (2) files in PDF format containing employee payroll information related to employee 2015 IRS W-2 forms, including employee Social Security Numbers, 2015 wages, 2015 taxes withheld, and amounts paid for other employee benefits. When the employee realized his error on approximately February 25, 2016, he reported the incident to Applied's IT department, which, together with Applied's senior leadership, including its CEO and General Counsel, immediately commenced an investigation into the incident and secured Applied against further disclosures of such information. The investigation confirmed no further disclosures of such information had been made.

Simultaneously, Applied removed the employee responsible for the errant disclosure from access to such information. Applied also began an investigation to determine how the incident occurred, and to determine what data and which individuals were involved. Applied has also investigated security measures to mitigate the likelihood of any future disclosures of this nature, including additional focus on security awareness and training.

Number of New Hampshire Residents Potentially Affected

Based on Applied's investigation, it has determined that one (1) New Hampshire resident was potentially affected under N.H. Rev. Stat. Ann. §§ 359-C:1.

Copy of the Notice Provided to the Affected Individual

Pursuant to N.H. Rev. Stat. Ann. §§ 359-C:1, on March 7, 2016, Applied mailed a letter to the affected New Hampshire resident notifying such resident of the incident. This notification letter is in the form of the letter attached.

Description of Any Services Being Offered to the Affected Individual Without Charge and Instructions on How to Use Such Services

The notification letter sent to the affected individual encourages him to take precautions to protect the security of his personal information, and also recommends remaining vigilant to prevent identity theft and fraud by monitoring credit reports, and financial institution and other account statements. The letter also provides a toll-free telephone number to call with any questions about the incident.

In addition, Applied is offering the affected resident two years of a free credit monitoring and identity theft protection product from Experian. Applied notified the affected resident how to enroll in the credit monitoring and identity theft protection service via the notification letter. To enroll, the individual will visit Experian's website and provide his personal activation code, which is listed in his individual notification letter.

Contact Information For Additional Information About the Incident

For any questions or additional information regarding this incident, please contact me or my partner, Bob Brewer, at:

Anthony J. McFarland
amcfarland@bassberry.com

Robert L. Brewer
rbrewer@bassberry.com

Bass, Berry & Sims PLC
150 Third Avenue South, Suite 2800
Nashville, TN 37201
615-742-6200 (phone)
615-742-6293 (fax)

Sincerely,

Anthony J. McFarland

AJM/16224586
Enclosure

Attachment A

March 7, 2016

<<First Name>> <<Last Name>>
<<Address Line 1>>
<<City>>, <<State>> <<Zip Code>>

Re: Unauthorized Disclosure of Personal Information

<<First Name>> <<Last Name>>:

On February 25, 2016, Applied Systems, Inc. ("Applied") learned that an employee of the company was targeted by an email "phishing" scheme on February 19 and that the employee unfortunately, and improperly, transmitted personal information outside the company by reply email. Specifically, certain information normally found on an employee IRS Form W-2 was attached to this email, which was sent in response to what appeared to the employee to be a legitimate request from an officer of Applied for that information. This information included:

1) Name;
2) Social Security Number;
3) 2015 wages paid;
4) 2015 taxes withheld;
5) states and municipalities where taxes were paid in 2015; and
6) amounts paid in 2015 for certain employee benefits.

Home address information was not included. And, to be clear, the following types of information were not disclosed:

1) dates of birth;
2) telephone numbers;
3) drivers' license numbers;
4) credit or debit card issuers or numbers;
5) bank names or account numbers;
6) family member names or information;
7) email addresses; or
8) personal medical or health information.

As soon as Applied discovered the attack, this employee's access to confidential information and all company systems was immediately suspended, and Applied began investigating whether any additional information was transmitted. Though the investigation is continuing, it does not appear that any other transmission of any other personal information or other data took place.

Individuals Impacted
All United States employees of Applied receiving an IRS Form W-2 from Applied for the 2015 calendar year were included. However, no information on any Applied employee in Canada or the

United Kingdom was involved, and individuals receiving only an IRS Form 1099 from Applied for the 2015 calendar year were not included.

Customers Not Impacted
No information of any customer of Applied was involved.

Company Information Technology Systems Not Impacted
To Applied's knowledge, this email phishing scheme did not intrude on Applied's information technology systems. None of Applied's internal systems, peer-hosted cloud infrastructure or customer information appears to have been compromised.

Identity Protection Services
To help protect your identity, Applied is offering you a **complimentary** two-year membership of Experian's® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **June 30, 2016** (Your code will not work after this date.)
2. VISIT the ProtectMyID Web Site to enroll: **www.protectmyid.com/enroll**
3. PROVIDE Your Activation Code: **<<Code>>**

If you have questions or need an alternative to enrolling online, please call 877-441-6943 and provide engagement #: **PC99674.**

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 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
  - **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
  - **Change of Address:** Alerts of any changes in your mailing address.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity 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.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

* 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.

Fraud Prevention Tips

Although Applied's investigation has not found that your information has been misused, Applied treats this matter with the utmost seriousness and wants you to have the information you need so you can take steps to try to help protect yourself from identity theft or fraud.

First, vigilantly monitor your account statements and your credit reports to spot any new accounts opened in your name, or fraudulent or unexplained activity under your current accounts. You can obtain a free copy of your credit report annually from each of the credit bureaus. By requesting a report from one bureau at a time over several months, you can get updated information throughout the year. Review your reports carefully to ensure the information is accurate. If you see anything on your credit reports or credit card account statements that appear incorrect, contact the credit reporting agency or your credit card provider, and report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission (FTC). Even if you do not find any signs of fraud on your reports or account statements, the FTC and other security experts suggest that you check your credit reports and account statements periodically.

Credit Bureau Information

Experian PO BOX 9532 ALLEN TX 75013 1-888-397-3742 experian.com	**Equifax** PO BOX 740241 ATLANTA GA 30374-0241 1-800-685-1111 equifax.com	**TransUnion** PO BOX 6790 FULLERTON CA 92834-6790 1-800-916-8800 transunion.com

Second, you can add a fraud alert to your credit report, making it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. However, a fraud alert on your account may delay your ability to obtain credit. You can also place a fraud alert in your file by calling any of the three nationwide credit bureaus listed below. As soon as that bureau processes your fraud alert, it will notify the other two bureaus, which then must also place fraud alerts in your file. A fraud alert lasts 90 days, and requires potential creditors to use "reasonable policies and procedures" to verify your identity before issuing credit in your name. You can keep the fraud alert in place at the credit reporting agencies by calling again after 90 days.

Experian fraud alert: 1-888-397-3742;
https://www.experian.com/fraud/center.html
Equifax fraud alert: 1-888-766-0008;
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

TransUnion fraud alert: 1-800-680-7289;
https://www.transunion.com/fraud-victim-resource/place-fraud-alert

Third, you can visit the credit bureau links below to see if and how you may place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your prior written authorization.

Experian security freeze: http://www.experian.com/consumer/security_freeze.html
Equifax security freeze:
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
TransUnion security freeze:
http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Fourth, you can find out information about the Internal Revenue Service's (IRS) fraud alert service at: https://www.irs.gov/pub/irs-pdf/f14039.pdf.

Fifth, you should report suspected incidents of identity theft to local law enforcement, the FTC, or your state Attorney General. To learn more from the FTC you can go to its web site (www.consumer.gov/idtheft), call their offices [1-877–ID-THEFT (438-4338); TTY: 1-866-653-4261] or write them [Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580].

It is Applied's understanding that in similar data breach incidents at other businesses, unscrupulous people have tried to further scam victims by sending emails that appear to come from that business (from Applied, for example). For instance, emails are sent to victims of a breach asking for personal information, and include a "click here" link for credit monitoring. You must continue to be vigilant. All notices regarding this incident will come directly from Applied, and all credit monitoring or identity protection notices will come from Experian.

Notification of Government Authorities
Some states require that they be notified when certain personal information is disclosed without authorization. Applied is preparing these notices, and will promptly send them out to the appropriate authorities.

We sincerely apologize that this incident occurred. Upon discovery, Applied began investigating measures to mitigate the likelihood of any future disclosures of this nature, including additional focus on security awareness and training. If you have questions about this letter or this incident, or need additional help, please contact Sunny Chauhan in Human Resources at schauhan@appliedsystems.com or 1-800-999-5368, extension 22022.