Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 10, 2017

VIA U.S. MAIL AND EMAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Pacific Science Center, 200 Second Avenue N, Seattle, WA 98109, and are writing to notify your office of an incident that may affect the security of personal information relating to approximately six hundred five (605) Washington residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Pacific Science Center does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Nature of the Data Event

Pacific Science Center was the victim of a "spear phishing" attack on June 13, 2017 and June 21, 2017 by an individual or individuals pretending to be a member of Pacific Science Center's management team. Unfortunately, copies of all 2016 employee W-2 forms were provided on both dates before the company discovered that the requests were fraudulent. Pacific Science Center discovered the fraudulent nature of the requests within hours and has been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to Washington Residents

On June 14, 2017, Pacific Science Center provided preliminary notice to current employees via email and/or hand delivery. A copy of this notice is attached hereto as ***Exhibit A***. On or about June 22, 2017, Pacific Science Center provided preliminary notice of the incident to former employees via U.S. mail. A copy of this preliminary notice is attached hereto as ***Exhibit B***. On July 10, 2017, Pacific Science Center will begin providing written notice of this incident to all affected current and former employees, which

includes approximately six hundred and five (605) Washington residents. Written notice will be provided in substantially the same form as the letters attached hereto as ***Exhibit C*** and ***Exhibit D***.

Other Steps Taken and To Be Taken

Upon discovering the fraudulent nature of the email, Pacific Science Center moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

Pacific Science Center is providing all potentially affected individuals access to three (3) free years of credit and identity monitoring services, including identity restoration services, through AllClear ID, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Pacific Science Center is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Pacific Science Center is also providing written notice of this incident to other state regulators as necessary.

Additionally, Pacific Science Center has provided notice of this incident to the IRS and the FBI.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4776.

Very truly yours,

Ed Finn of

MULLEN COUGHLIN LLC

EJF:am

Cc: Office of the Attorney General, Consumer Protection Division

Exhibit A

[redacted]

From: [redacted]
Sent: Wednesday, June 14, 2017 8:05 PM
To: [redacted]
Subject: Important Message - Please Read
Attachments: Form 14039 (Rev.pdf

Importance: High

Dear Pacific Science Center colleagues,

We were dismayed yesterday to learn that unauthorized parties have obtained the 2016 W-2 information of everyone who received a paycheck from Pacific Science Center in 2016. We have notified the FBI. We are also taking steps to strengthen internal processes and defenses to protect our confidential information. It appears that one of our employees received and responded to an email that appeared to come from our management requesting copies of 2016 W-2 forms. We don't have any indication that anyone from our own team was intentionally involved in the theft of this information from us. We don't have all the answers yet, but please direct any questions you have about this breach to Chris Wheaton, Linda Freeburg, or me. Discussing this issue casually or with anyone other than Chris, Linda, or me could make it harder for us to do our work in support of the investigation, so please do not discuss this data breach with anyone other than us.

We realize this news is likely upsetting and/or frustrating. We also recognize that it is an unfortunate reality of our modern digital world. What is important now is for us to do our best to keep data thieves from using the names, addresses, and social security numbers contained in our W-2s in IRS tax fraud or general identity theft.

Towards that end, we want each of you to take the steps outlined at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft as quickly as possible. Here's a quick summary for handy reference:

1. Report identity theft to the Federal Trade Commission at https://www.identitytheft.gov/, where you will be asked to choose an option best describing the situation. For example, if you have received a notice that an unauthorized tax return has been filed in your name you would select "someone else filed a tax return using my information." If that option does not apply to you and you are unaware of any misuse of your personal information, you may choose the option "someone got my personal information or my wallet, and I'm worried about identity theft" to describe the situation.
2. Contact one of the three credit bureaus to place either a Credit Freeze or a Fraud Alert on your credit file. https://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes#credit
3. If you have any issue when filing your federal income taxes such as a rejection because of duplicate filing under your SSN, Report this to us so that we may inform the FBI.
4. To put a notice on your file with the IRS to be alert to fraud, or if your tax return is rejected for duplicate filing, complete and submit the IRS Form 14039 https://www.irs.gov/pub/irs-pdf/f14039.pdf
    a. Section A: Check box 1.

b. Section B: If your income tax return was rejected for duplicate filing, check box 1. If your income tax return has not been rejected for duplicate filing, check box 2.
c. The following text may be used where the form asks for a description of the issue: "I was advised by my employer that my W2 information has been obtained by an unauthorized third party." Instructions on submitting the form are on page 2 of the form.

Filing the form alone automatically protects the tax account and the IRS will monitor the account for any fraudulent activities. For an extra layer of security, include a request in the explanation section of the 14039 to have a PIN assigned.

5. Pacific Science Center will provide each of you with a credit monitoring service that will alert you to changes in your credit profile. This service will be at no cost to you. You will receive a letter by US mail with instructions on how to enroll in the credit monitoring service.

Again, we understand that this news is likely upsetting and/or frustrating. The good news is that there are several ways to protect yourself. We will be sharing more information about how employees can protect themselves as it becomes available. HR will be available to help employees consider how to navigate these steps.

If you have any further questions or just want to talk, please reach out to Chris Wheaton, Linda Freeburg, or me. We will do everything we can to help.

Sincerely,
Will

Will Daugherty | PACIFIC SCIENCE CENTER
President & CEO | Office +1.206.443.2889 | Mobile +1.206.369.9811
Pacific Science Center is an independent not-for-profit institution that ignites curiosity and fuels a passion for discovery, experimentation, and critical thinking

Exhibit B

June 21, 2017

Dear former employees of Pacific Science Center,

We were dismayed last week to learn that unauthorized parties have obtained the 2016 W-2 information of everyone who received a paycheck from Pacific Science Center in 2016. We have notified the FBI. We are also taking steps to strengthen internal processes and defenses to protect our confidential information. It appears that one of our employees received and responded to an email that appeared to come from our management requesting copies of 2016 W-2 forms.

We realize this news is likely upsetting and/or frustrating. We also recognize that it is an unfortunate reality of our modern digital world. What is important now is for us to do our best to keep data thieves from using the names, addresses, and social security numbers contained in our W-2s in IRS tax fraud or general identity theft.

Towards that end, we recommend you take the steps outlined at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft as quickly as possible. Here is a quick summary for handy reference:

1. Report identity theft to the Federal Trade Commission at https://www.identitytheft.gov/, where you will be asked to choose an option best describing the situation. For example, if you have received a notice that an unauthorized tax return has been filed in your name you would select "someone else filed a tax return using my information." If that option does not apply to you and you are unaware of any misuse of your personal information, you may choose the option "someone got my personal information or my wallet, and I'm worried about identity theft" to describe the situation.
2. Contact one of the three credit bureaus to place either a Credit Freeze or a Fraud Alert on your credit file. https://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes#credit
3. If you have any issue when filing your federal income taxes such as a rejection because of duplicate filing under your SSN, report this to us so that we may inform the FBI.
4. To put a notice on your file with the IRS to be alert to fraud, or if your tax return is rejected for duplicate filing, complete and submit the IRS Form 14039 https://www.irs.gov/pub/irs-pdf/f14039.pdf. According to the IRS, filing the form alone automatically protects the tax account and the IRS will monitor the account for any fraudulent activities. For an extra layer of security, include a request in the explanation section of the 14039 to have a PIN assigned.
5. Pacific Science Center will provide each affected person with the option to enroll in a credit monitoring service that will alert you to changes in your credit profile. This service will be at no cost to you. You will receive a letter by US mail with instructions on how to enroll in the credit monitoring service.

We deeply regret that this incident occurred and are committed to making improvements in our procedures and practices to prevent this type of incident in the future.

Sincerely,

Will Daugherty

Will Daugherty
President & CEO

PACIFIC SCIENCE CENTER

200 Second Avenue N
Seattle, Washington
98109-4895

(206) 443-2001
pacificsciencecenter.org

Pacific Science Center ignites curiosity in every child and fuels a passion for discovery, experimentation, and critical thinking in all of us.

Exhibit C

PACIFIC SCIENCE CENTER
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00001
00001
ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

[redacted]

Re: Notice of Data Breach

Dear John Sample:

We are writing to provide you with additional information related to the recent theft of employee W-2 data that may affect the security of your personal information. We take this incident very seriously and, as promised, are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? Pacific Science Center was the victim of a "spear phishing" attack on June 13, 2017 and June 21, 2017 by an individual pretending to be a member of our management team. On both dates, this individual successfully obtained copies of all 2016 employee W-2 forms before we discovered that the requests were fraudulent. We discovered the fraudulent nature of the attacks within hours and have been working tirelessly to investigate and to mitigate the impact of the attacks.

What Information Was Involved? A file, including a copy of your IRS Tax Form W-2, was emailed in response to the fraudulent requests. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Pacific Science Center has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individual(s) who sent the fraudulent emails accessed our computer network or that our IT systems were otherwise compromised by this attack. However, our IT and CyberSecurity teams are assessing the security and soundness of our systems. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have notified the IRS and FBI, and will be contacting the relevant state Attorneys General.

As an added precaution, we have arranged to have AllClear ID protect your identity for 36 months at no cost to you. The cost of this service will be paid for by Pacific Science Center. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the monitoring service.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-361-3675 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-361-3675 using the following redemption code: Redemption Code.

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

What You Can Do. You can review the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud*. You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-361-3675 (toll free), Monday through Saturday, 6:00 a.m. to 6:00 p.m. PT.

Pacific Science Center takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Will Daugherty
President & CEO

Enclosure

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

Exhibit D

PACIFIC SCIENCE CENTER
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00615
TO THE PARENT OR GUARDIAN OF
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

00003
ACD1234

[redacted]

Re: Notice of Data Breach

Dear Parent or Guardian of John Sample:

We are writing to provide you with additional information related to the recent theft of employee W-2 data that may affect the security of your minor child's personal information. We take this incident very seriously and, as promised, are providing you with information and access to resources to protect your minor child's personal information, should you feel it is appropriate to do so.

What Happened? Pacific Science Center was the victim of a "spear phishing" attack on June 13, 2017 and June 21, 2017 by an individual pretending to be a member of our management team. On both dates, this individual successfully obtained copies of all 2016 employee W-2 forms before we discovered that the requests were fraudulent. We discovered the fraudulent nature of the attacks within hours and have been working tirelessly to investigate and to mitigate the impact of the attacks.

What Information Was Involved? A file, including a copy of your minor child's IRS Tax Form W-2, was emailed in response to the fraudulent requests. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Pacific Science Center has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individual(s) who sent the fraudulent emails accessed our computer network or that our IT systems were otherwise compromised by this attack. However, our IT and CyberSecurity teams are assessing the security and soundness of our systems. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have notified the IRS and FBI, and will be contacting the relevant state Attorneys General.

As an added precaution, we have arranged to have AllClear ID protect your minor child's identity for 36 months at no cost to you. The cost of this service will be paid for by Pacific Science Center. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months. It is incumbent upon you to enroll your minor child in these services, as we are not able to act on your behalf to enroll your minor child in the monitoring service.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-361-3675 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-361-3675 using the following redemption code: Redemption Code.

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

What You Can Do. You can review the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud*. You can also enroll your minor child to receive the free monitoring and identity restoration services described above. In addition, if your minor child is required to, and has not already done so, we encourage your minor child to file their 2016 tax return as soon as possible.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-361-3675 (toll free), Monday through Saturday, 6:00 a.m. to 6:00 p.m. PT.

Pacific Science Center takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you and your minor child.

Sincerely,

Will Daugherty
President & CEO

Enclosure

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect your minor child against possible identity theft or financial loss.

We encourage your minor child to file their 2016 tax return as soon as possible, if they are required to and have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your minor child's name and what to do if your minor child becomes the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your minor dependent's account statements, and to monitor your minor dependent's credit report to ensure credit has not been granted in his or her name. While minors do not have credit files, the following information relates to protecting one's credit once established:

Under U.S. law, adults with credit files are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of a credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on a credit file that alerts creditors to take additional steps to verify identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect identity, it may also delay one's ability to obtain credit while the agency verifies identity. As soon as one credit bureau confirms the fraud alert, the others are notified to place fraud alerts on the credit file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself and your dependent, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261.

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General.