<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Breach

Dear <<FTC>> <<MemberMiddleName>> <<LTC>>,

Adams 12 Five Star Schools ("Adams 12") is writing to advise you of an event that may impact the security of your personal information. While we are unaware of any attempted or actual misuse of your data, we are providing you with information about the event, our response to the event, steps we are taking to enhance our data protection, and resources you may take advantage of to further protect against the possible misuse of your information, should you feel it appropriate to do so.

What Happened?
Earlier this year, Adams 12 became aware of unusual activity from an outside source accessing an Adams 12 employee's email account. We immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third-party forensic investigators, we determined that certain employee email accounts were subject to unauthorized access from outside sources between February 15, and February 19, 2019. Because the initial assessment was unable to identify what, if any, emails were viewed without authorization, we began an extensive investigation to understand all information within the email accounts that was potentially accessible. Following a thorough and resource-intensive review of the contents of the accounts, on June 12, 2019, Adams 12 determined that the accounts subject to unauthorized access contained protected information of certain individuals, including you.

Based upon available forensic evidence, Adams 12 was unable to confirm whether the email or document containing your information was actually viewed by an unauthorized user. Our investigation was only able to determine your information was present in emails and/or attachments in the email accounts subject to unauthorized access.

What Information Was Involved?
The email accounts subject to unauthorized access contained the following types of information relating to you: your <<ClientDef1>><<ClientDef2>>. To date, we have not received any reports of actual or attempted misuse of personal information potentially affected by this incident.

What We Are Doing.
We take this incident and the security of personal information very seriously. Upon discovering unusual activity in our system, we immediately took steps to restore our network and conducted an investigation to determine how this incident occurred and who may be affected. This investigation included working with third-party forensic experts to confirm the nature and scope of the incident. Additionally, while we have safeguards in place to protect data in our care, we are working to review and enhance these protections as part of our ongoing commitment to data security.

What You Can Do.
We encourage you to review the information in the enclosed *Steps You Can Take To Protect Personal Information* and to take advantage of fraud consultation and identity theft restoration services we are offering, should they become necessary.

For More Information
Should you have questions about this incident that are not addressed in this letter, please call our dedicated assistance line at 1-866-775-4209. Representatives are available Monday through Friday, during the hours of 8:00 a.m. to 5:30 p.m., Central Time.

Again, we take the privacy and security of the personal information in our care seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Ash Mahajan

Ash Mahajan
Chief Information & Technology Officer
Adams 12 Five Star Schools

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

We have secured the services of Kroll to provide Fraud Consultation and Identity Theft Restoration services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your Membership Number is: **<<Member ID>>**

Additional information describing your services is included with this letter.

Monitor Accounts, Financial and Medical Billing Statements

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, medical bills, explanation of benefits (EOBs), and credit reports for suspicious charges or claims. 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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order 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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, 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); 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov <http://www.ncdoj.gov/>

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF FRAUD CONSULTATION AND IDENTITY THEFT RESTORATION SERVICES

You've been provided with access to the following services from Kroll:

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

<<Date>> (Format: Month Day, Year)

To the Parent(s) and/or Guardian(s) of:
<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Breach

To the Parent(s) and/or Guardian(s) of <<FTC>> <<MemberMiddleName>> <<LTC>>,

Adams 12 Five Star Schools ("Adams 12") is writing to advise you of an event that may impact the security of your child's personal information. While we are unaware of any attempted or actual misuse of their data, we are providing you with information about the event, our response to the event, steps we are taking to enhance our data protection, and resources you may take advantage of, to further protect against the possible misuse of their information, should you feel it appropriate to do so.

What Happened?
Earlier this year, Adams 12 became aware of unusual activity from an outside source accessing an Adams 12 employee's email account. We immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third-party forensic investigators, we determined that certain employee email accounts were subject to unauthorized access from outside sources between February 15, and February 19, 2019. Because the initial assessment was unable to identify what, if any, emails were viewed without authorization, we began an extensive investigation to understand all information within the email accounts that was potentially accessible. Following a thorough and resource-intensive review of the contents of the accounts, on June 12, 2019, Adams 12 determined that the accounts subject to unauthorized access contained protected information of certain individuals, including your child.

Based upon available forensic evidence, Adams 12 was unable to confirm whether the email or document containing your child's information was actually viewed by an unauthorized user. Our investigation was only able to determine your child's information was present in emails and/or attachments in the employee email accounts subject to unauthorized access.

What Information Was Involved?
The email accounts subject to unauthorized access contained the following types of information relating to your child: their <<ClientDef1>><<ClientDef2>>. To date, we have not received any reports of actual or attempted misuse of personal information potentially affected by this incident.

What We Are Doing.
We take this incident and the security of personal information very seriously. Upon discovering unusual activity in our system, we immediately took steps to restore our network and conducted an investigation to determine how this incident occurred and who may be affected. This investigation included working with third-party forensic experts to confirm the nature and scope of the incident. Additionally, while we have safeguards in place to protect data in our care, we are working to review and enhance these protections as part of our ongoing commitment to data security.

What You Can Do.
We encourage you to review the information in the enclosed *Steps You Can Take To Protect Personal Information*.

For More Information
Should you have questions about this incident that are not addressed in this letter, please call our dedicated assistance line at 1-866-775-4209. Representatives are available Monday through Friday, during the hours of 8:00 a.m. to 5:30 p.m., Central Time.

Again, we take the privacy and security of the personal information in our care seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Ash Mahajan

Ash Mahajan
Chief Information & Technology Officer
Adams 12 Five Star Schools

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

We have secured the services of Kroll to provide Fraud Consultation and Identity Theft Restoration services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your Child's Membership Number is: **<<Member ID>>**

Additional information describing your services is included with this letter.

Monitor Accounts, Financial and Medical Billing Statements

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your child's account statements, medical bills, explanation of benefits (EOBs), and your credit reports for suspicious charges or claims. 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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order 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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, 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); 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF FRAUD CONSULTATION AND IDENTITY THEFT RESTORATION SERVICES

You've been provided with access to the following services from Kroll:

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your child's identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If your child becomes a victim of identity theft, an experienced Kroll licensed investigator will work on their behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your child's investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.