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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Mater Dei High School ("Mater Dei") is writing to inform you of a recent cybersecurity incident that may have resulted in an unauthorized access of some of your sensitive personal information. While we are unaware of any misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and free resources available to help you protect your information.

What Happened?

In late January 2021, Mater Dei became aware of suspicious logins into some of its employees' email accounts likely due to a response to a phishing email message with a malicious link. Upon discovery of this incident, Mater Dei engaged cyber counsel and a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation confirmed that two of Mater Dei employees' accounts had unauthorized access from January 1, 2021 to March 4, 2021 where information could have been viewed or exfiltrated. Once the unauthorized access was confirmed, Mater Dei promptly engaged a third party vendor to review all the files and emails within the compromised email accounts to identify the potentially impacted individuals whose information may have been exposed during the period of unauthorized access. This investigation concluded early June 2021, and it determined that your personal information was within one of the compromised accounts. Since then, Mater Dei has been working internally to identify the addresses for these individuals to send you this notice. At this time, Mater Dei has no reason to believe your personal information has been misused by any third parties. However, out of an abundance of caution, we wanted to inform you of this incident.

What Information Was Involved?

The types of information involved varied by individual, and very few individuals had every field of data impacted. However, the information potentially exposed during the unauthorized access may have included your name, address, Social Security number, driver's license number, passport number, credit card number with security code and expiration date, Identity Protection PIN, full access credentials to FACTS, and/or protected health information, including but not limited to diagnosis, treatment and prescription information, provider name, patient ID, Medicare/Medicaid number, health insurance information, and treatment cost.

What We Are Doing

Mater Dei is committed to ensuring the security of all personal information in our control. As mentioned above, upon discovery of this incident, we engaged cyber counsel and a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. We also changed all email passwords, improved our computer security settings, and new policies were implemented to reduce the storage of sensitive personal information within our email systems. Additionally, we are providing you with guidance on how to help protect against the possibility of information misuse.

Our objective is to always help protect your personal information, and to assist to that end, we are providing you with 12 months of complimentary identity monitoring services through Kroll. While we are covering the cost of these services, you will need to complete the activation process by following the instructions included in the enclosed *Steps You Can Take to Help Protect Your Information.*

Again, based on available evidence through monitoring, we are not aware of your information being used in an unauthorized manner, but we nonetheless encourage you to activate the free identity monitoring services to provide peace of mind and additional protection.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. You may also wish to consider changing your passwords to important online accounts. We also caution you to **never assume** an email message requesting you to redirect your payments due the school to another unknown account be acted upon without first checking with Mater Dei as to the validity of the message. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the identity monitoring services we are making available to you. Again, while we are providing these services to you at no cost, you will need to activate these services yourself. The activation deadline is November 9, 2021.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-XXX-XXX-XXXX (toll free) during the hours of 8:00 AM a.m. and 5:30 PM p.m. Central Standard Time, Monday through Friday (excluding U.S. national holidays).

Mater Dei sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Mater Dei High School

Steps You Can Take to Help Protect Your Information

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring 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 identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **November 9, 2021** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single Bureau Credit Monitoring: You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

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 can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

More information can also be obtained by contacting the Federal Trade Commission:

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon*, and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission – Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General – Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General – Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General – 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General – Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General – Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General – Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General – Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov

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

<<b2b_text_1(BusinessName)>>
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Mater Dei High School ("Mater Dei") is writing to inform you of a recent cybersecurity incident that may have resulted in an unauthorized access of some of your sensitive personal information. While we are unaware of any misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and free resources available to help you protect your information.

What Happened?

In late January 2021, Mater Dei became aware of suspicious logins into some of its employees' email accounts likely due to a response to a phishing email message with a malicious link. Upon discovery of this incident, Mater Dei engaged cyber counsel and a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation confirmed that two of Mater Dei employees' accounts had unauthorized access from January 1, 2021 to March 4, 2021 where information could have been viewed or exfiltrated. Once the unauthorized access was confirmed, Mater Dei promptly engaged a third party vendor to review all the files and emails within the compromised email accounts to identify the potentially impacted individuals whose information may have been exposed during the period of unauthorized access. This investigation concluded early June 2021, and it determined that your personal information was within one of the compromised accounts. Since then, Mater Dei has been working internally to identify the addresses for these individuals to send you this notice. At this time, Mater Dei has no reason to believe your personal information has been misused by any third parties. However, out of an abundance of caution, we wanted to inform you of this incident.

What Information Was Involved?

The information potentially exposed during the unauthorized access may have included your business name, address, and full access credentials to FACTS.

What We Are Doing

Mater Dei is committed to helping ensure the security of all personal information in our control. As mentioned above, upon discovery of this incident, we engaged cyber counsel and a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. We also changed all email passwords, improved our computer security settings, and new policies were implemented to reduce the storage of sensitive personal information within our email systems. Additionally, we are providing you with guidance on how to help protect against the possibility of information misuse.

Again, based on available evidence through monitoring, we are not aware of your information being used in an unauthorized manner.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. You

may also wish to consider changing your passwords to important online accounts. We also caution you to **never assume** an email message requesting you to redirect your payments due the school to another unknown account be acted upon without first checking with Mater Dei as to the validity of the message. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-XXX-XXX-XXXX (toll free) during the hours of 8:00 AM a.m. and 5:30 PM p.m. Central Standard Time, Monday through Friday (excluding U.S. national holidays).

Mater Dei sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Mater Dei High School

Steps You Can Take to Help Protect Your Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

More information can also be obtained by contacting the Federal Trade Commission:

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon,* and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission – Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General – Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General – Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General – 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General – Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General – Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General – Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General – Consumer Protection: 150 South Main St., Providence RI 02903**;** 1-401-274-4400**;** www.riag.ri.gov

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Mater Dei High School ("Mater Dei") is writing to inform you of a recent cybersecurity incident that may have resulted in an unauthorized access of some of your sensitive personal information. While we are unaware of any misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and free resources available to help you protect your information.

What Happened?

In late January 2021, Mater Dei became aware of suspicious logins into some of its employees' email accounts likely due to a response to a phishing email message with a malicious link. Upon discovery of this incident, Mater Dei engaged cyber counsel and a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation confirmed that two of Mater Dei employees' accounts had unauthorized access from January 1, 2021 to March 4, 2021 where information could have been viewed or exfiltrated. Once the unauthorized access was confirmed, Mater Dei promptly engaged a third party vendor to review all the files and emails within the compromised email accounts to identify the potentially impacted individuals whose information may have been exposed during the period of unauthorized access. This investigation concluded early June 2021, and it determined that your personal information was within one of the compromised accounts. Since then, Mater Dei has been working internally to identify the addresses for these individuals to send you this notice. At this time, Mater Dei has no reason to believe your personal information has been misused by any third parties. However, out of an abundance of caution, we wanted to inform you of this incident.

What Information Was Involved?

The information potentially exposed during the unauthorized access may have included your business name, address, tax ID number and Identity Protection PIN.

What We Are Doing

Mater Dei is committed to helping ensure the security of all personal information in our control. As mentioned above, upon discovery of this incident, we engaged cyber counsel and a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. We also changed all email passwords, improved our computer security settings, and new policies were implemented to reduce the storage of sensitive personal information within our email systems. Additionally, we are providing you with guidance on how to help protect against the possibility of information misuse.

Again, based on available evidence through monitoring, we are not aware of your information being used in an unauthorized manner.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. You

may also wish to consider changing your passwords to important online accounts. We also caution you to **never assume** an email message requesting you to redirect your payments due the school to another unknown account be acted upon without first checking with Mater Dei as to the validity of the message. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-XXX-XXX-XXXX (toll free) during the hours of 8:00 AM a.m. and 5:30 PM p.m. Central Standard Time, Monday through Friday (excluding U.S. national holidays).

Mater Dei sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Mater Dei High School

Steps You Can Take to Help Protect Your Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

More information can also be obtained by contacting the Federal Trade Commission:

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon,* and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission – Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General – Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General – Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General – 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General – Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General – Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General – Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General – Consumer Protection: 150 South Main St., Providence RI 02903**;** 1-401-274-4400**;** www.riag.ri.gov

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

<<b2b_text_1(BusinessName)>>
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Mater Dei High School ("Mater Dei") is writing to inform you of a recent cybersecurity incident that may have resulted in an unauthorized access of some of your sensitive personal information. While we are unaware of any misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and free resources available to help you protect your information.

What Happened?

In late January 2021, Mater Dei became aware of suspicious logins into some of its employees' email accounts likely due to a response to a phishing email message with a malicious link. Upon discovery of this incident, Mater Dei engaged cyber counsel and a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation confirmed that two of Mater Dei employees' accounts had unauthorized access from January 1, 2021 to March 4, 2021 where information could have been viewed or exfiltrated. Once the unauthorized access was confirmed, Mater Dei promptly engaged a third party vendor to review all the files and emails within the compromised email accounts to identify the potentially impacted individuals whose information may have been exposed during the period of unauthorized access. This investigation concluded early June 2021, and it determined that your personal information was within one of the compromised accounts. Since then, Mater Dei has been working internally to identify the addresses for these individuals to send you this notice. At this time, Mater Dei has no reason to believe your personal information has been misused by any third parties. However, out of an abundance of caution, we wanted to inform you of this incident.

What Information Was Involved?

The information potentially exposed during the unauthorized access may have included your name, address, and tax ID number.

What We Are Doing

Mater Dei is committed to ensuring the security of all personal information in our control. As mentioned above, upon discovery of this incident, we engaged cyber counsel and a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. We also changed all email passwords, improved our computer security settings, and new policies were implemented to reduce the storage of sensitive personal information within our email systems. Additionally, we are providing you with guidance on how to help protect against the possibility of information misuse.

Our objective is to always help protect your personal information, and to assist to that end, we are providing you with 12 months of complimentary identity monitoring services through Kroll. While we are covering the cost of these services, you will need to complete the activation process by following the instructions included in the enclosed *Steps You Can Take to Help Protect Your Information.*

Again, based on available evidence through monitoring, we are not aware of your information being used in an unauthorized manner, but we nonetheless encourage you to activate the free identity monitoring services to provide peace of mind and additional protection.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. You may also wish to consider changing your passwords to important online accounts. We also caution you to **never assume** an email message requesting you to redirect your payments due the school to another unknown account be acted upon without first checking with Mater Dei as to the validity of the message. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the identity monitoring services we are making available to you. Again, while we are providing these services to you at no cost, you will need to activate these services yourself. The activation deadline is November 9, 2021.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1-XXX-XXX-XXXX (toll free) during the hours of 8:00 AM a.m. and 5:30 PM p.m. Central Standard Time, Monday through Friday (excluding U.S. national holidays).

Mater Dei sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Mater Dei High School

Steps You Can Take to Help Protect Your Information

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring 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 identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **November 9, 2021** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single Bureau Credit Monitoring: You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

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 can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

More information can also be obtained by contacting the Federal Trade Commission:

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon*, and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission – Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General – Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General – Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General – 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General – Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General – Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General – Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General – Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov