Appendix

Shattuck-St. Mary's is a private boarding and day school in Faribault, Minnesota. It completed an investigation into suspicious activity originating from one Shattuck-St. Mary's employee account. Upon discovery of the activity, Shattuck-St. Mary's immediately took measures to secure the account and began an investigation with the assistance of a computer forensic firm. The investigation determined that the unauthorized person not associated with Shattuck-St. Mary's accessed the email account at least once on May 13, 2020, but no later than May 15, 2020. The unauthorized person created a rule whereby certain emails were forwarded to an unknown email address. Shattuck-St. Mary's removed this rule as soon as it was discovered. The investigation did not determine whether any of the forwarded emails or attachments, or any other emails or attachments in the account, were viewed by the unauthorized person; however, Shattuck-St. Mary's reviewed all of the emails and attachments in the account to identify individuals whose information may have been accessible to the unauthorized person. On October 19, 2020, Shattuck-St. Mary's determined that an email or attachment in the account contained the name and one or more of the following data elements belonging to seven residents of Maine: Social Security number, financial account number and/or payment card number.

Beginning today, January 8, 2021, Shattuck-St. Mary's will mail notification letters via First-Class U.S. mail to the seven Maine residents.[1] A sample copy of the notification letter is enclosed. Shattuck-St. Mary's is offering the Maine residents with a Social Security number involved one year of complimentary credit monitoring, fraud consultation, and identity theft restoration services through Kroll. Shattuck-St. Mary's has established a dedicated phone number that individuals may call with related questions.

To further protect personal information, Shattuck-St. Mary's has incorporated additional authentication measures for remote email access, implemented additional data security measures, and provided re-education to its staff for awareness on these types of incidents.

[1] This notice is not, and does not constitute, a waiver of Shattuck-St. Mary's objection that Maine lacks personal jurisdiction over it regarding any claims related to this data security incident.

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

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

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

At Shattuck-St. Mary's School, we recognize the importance of securing and protecting personal information. However, all organizations face security risks. I am writing to inform you of an incident that involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

We recently completed an investigation into suspicious activity originating from one Shattuck-St. Mary's employee's email account. As soon as we became aware of the activity, we immediately took measures to secure the account and launched an investigation with the assistance of a computer forensic firm. The investigation determined that an unauthorized person not associated with Shattuck-St. Mary's accessed one employee email account at least once on May 13, 2020, but no later than May 15, 2020, and created a rule whereby certain emails were forwarded to an unknown email address. We removed the rule as soon as we became aware of it.

The investigation did not determine whether any of the forwarded emails or attachments, or any other emails or attachments in the account, were viewed by the unauthorized person; however, we were not able to rule out that possibility. In an abundance of caution, we searched the full contents of the account to identify individuals whose information may have been accessible to the unauthorized person. On October 19, 2020, we determined that an email or attachment in the account included your <<b2b_text_1 (Impacted Data)>>.

While we have no indication that your information was actually viewed by the unauthorized person, or that it has been misused, we wanted to notify you of this incident and assure you that we take it very seriously. We encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. As an added precaution, we have secured the services of Kroll, a cybersecurity services firm, to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **March 31, 2021** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

For more information on how to help safeguard your identity, steps you can take to help protect your personal information, and your complimentary one-year identity monitoring membership, please see the attached information provided in this letter.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect personal information, we have added additional authentication measures for remote email access, implemented additional data security measures, and provided re-education to our staff for awareness on these types of incidents. If you have any questions, please call 1-???-???-????, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time, excluding major US holidays.

Sincerely,

Scott J. Ryberg
CFO
Shattuck-St. Mary's

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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.

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

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

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

At Shattuck-St. Mary's School, we recognize the importance of securing and protecting personal information. However, all organizations face security risks. I am writing to inform you of an incident that involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

We recently completed an investigation into suspicious activity originating from one Shattuck-St. Mary's employee's email account. As soon as we became aware of the activity, we immediately took measures to secure the account and launched an investigation with the assistance of a computer forensic firm. The investigation determined that an unauthorized person not associated with Shattuck-St. Mary's accessed one employee email account at least once on May 13, 2020, but no later than May 15, 2020, and created a rule whereby certain emails were forwarded to an unknown email address. We removed the rule as soon as we became aware of it.

The investigation did not determine whether any of the forwarded emails or attachments, or any other emails or attachments in the account, were viewed by the unauthorized person; however, we were not able to rule out that possibility. In an abundance of caution, we searched the full contents of the account to identify individuals whose information may have been accessible to the unauthorized person. On October 19, 2020, we determined that an email or attachment in the account included your <<b2b_text_1 (Impacted Data)>>.

While we have no indication that your information was actually viewed by the unauthorized person, or that it has been misused, we wanted to notify you of this incident and assure you that we take it very seriously. We encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. For more information on identity theft prevention and steps you can take to help protect your personal information, please see the attached additional information provided in this letter.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect personal information, we have added additional authentication measures for remote email access, implemented additional data security measures, and provided re-education to our staff for awareness on these types of incidents. If you have any questions, please call 1-???-???-????, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time, excluding major US holidays.

Sincerely,

Scott J. Ryberg
CFO
Shattuck-St. Mary's

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov