



April 30, 2020

**Via U.S. Mail**

[Insert Name]  
[Insert Address]

Dear [Insert Name]:

We are contacting you about a recent data breach at Sisters of the Presentation of the Blessed Virgin Mary of Aberdeen, South Dakota (“Presentation”) that may affect the security of your personal information. Although we are not aware of any misuse of your information, we are providing this notice to ensure that you are aware of the incident so that you may take steps to protect your information should you feel it is appropriate to do so.

In early March 2020, Presentation discovered that unauthorized actors outside of Presentation obtained access to an employee’s email account through a phishing attack and may have subsequently gained access to Presentation’s computer network. As a result of the relationship between Presentation and Avera-St. Luke’s (“Avera”), certain information may have been exchanged between Presentation and Avera. Such information may have contained our personal information and may have been exposed as a result of the data breach. While we cannot be certain what specific files or information was accessed, the unauthorized actors may have accessed files that contained your name, address, social security number, account numbers, and other financial information.

We take the security of your personal information very seriously. After discovering this breach, Presentation immediately began with an internal security lockdown effort. We also promptly retained a cybersecurity company and law firm to implement measures to stop this unauthorized access and conduct a forensic examination to determine the extent of the breach. Following this incident, we have made changes to our data storage environment and security procedures to decrease the chance of a similar occurrence in the future. At this time, we are not aware of any fraudulent or improper use of your personal information, nor are we aware of any subsequent disclosure of your data, but to be cautious, we are providing this notice to you. Please be assured that we have taken every step necessary to address the incident to date, and that we will continue to investigate and take any additional steps that may be required to ensure your personal information is protected.

As a precautionary measure, we are providing you with identity theft protection and mitigation services from LifeLock, including credit monitoring, for twelve (12) months at no cost. Please contact us if you would like to enroll. You should also place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com or 1-800-685-1111

Experian: experian.com or 1-888-397-3742

TransUnion: transunion.com or 1-888-909-8872

You can also request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a free credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name.

If your personal information has been misused, visit the FTC's site at [IdentityTheft.gov](http://IdentityTheft.gov) to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations. This website also recommends steps that you can take to help protect yourself from identity theft, depending on the type of information exposed.

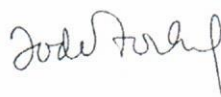
We also encourage you to review *Identity Theft: A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft which is available at: [https://www.consumer.ftc.gov/articles/pdf-0009\\_identitytheft\\_a\\_recovery\\_plan.pdf](https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf).

On behalf of everyone at Presentation, we sincerely apologize for this incident and any inconvenience it may cause. Your trust and the safeguarding of your personal information are of paramount importance to Presentation. Should you have any questions or concerns regarding this matter or the protections available, please feel free to call us at 605-229-8447 or email us directly at [jbierle@presentationsisters.org](mailto:jbierle@presentationsisters.org).

Sincerely,



Sister Janice Klein  
President, Presentation Sisters



Todd Forkel  
CEO, Avera St. Luke's