

Via Electronic Mailsecuritybreach@atq.wa.gov

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Notice of Security Incident

Dear Attorney General Ferguson:

We are writing you on behalf of our client the Wisconsin Evangelical Lutheran Synod, N16W23377 Stone Ridge Drive, Waukesha, WI 53188-1108 (“WELS”) through its attorneys Michael Best & Friedrich, LLP, 1 S. Pinckney St., Ste. 700, Madison, WI 53703 (“MBF”), to update about a data breach that occurred at Blackbaud, one of WELS’ third-party service providers. This notice is a supplement to the one previously provided to you on or about August 10, 2020, relating to the same Blackbaud incident described therein. The Wisconsin Evangelical Lutheran Synod (“WELS”) operates Martin Luther College, the Michigan Lutheran Seminary, and the Wisconsin Lutheran Seminary (collectively, the “Educational Institutions”), and WELS engages Blackbaud for various services to help manage its donations and constituent communications and other services that help the Educational Institutions manage their student information.

Martin A. Spriggs WELS Chief Technology Officer Data Protection Officer, martin.spriggs@wels.net, (414) 256-3250, is WELS’ contact, and Adrienne S. Ehrhardt, Partner, asehrhardt@michaelbest.com, (608) 283-0131, from MBF is WELS’ legal counsel, assisting with the management of this incident.

On July 16, 2020, Blackbaud notified WELS that it suffered a ransomware attack in May 2020, which it successfully stopped. At that time, Blackbaud assured WELS that the security incident was limited in scope and did not involve unencrypted sensitive information such as Social Security Number but that it did involve unencrypted date of birth. WELS responded appropriately and notified the affected individuals and also sent you the August 10, 2020 notice. On or about September 29, 2020, however, Blackbaud notified WELS that it discovered that the incident impacted old unused tables from legacy services that WELS no longer uses, containing sensitive unencrypted information relating to WELS and its Educational Institutions. Blackbaud acknowledged that neither WELS nor its Educational Institutions had any knowledge of the existence of these old tables.

Blackbaud now informs us that the personal information that may have been accessed may include name, date of birth, financial account number, and Social Security Number. After receiving the list of affected individuals from Blackbaud, on or about October 15, 2020, WELS determined the Social Security Numbers of 89 Washington state residents were impacted.

November 6, 2020
Page 2


Blackbaud explained in its initial notice to WELS that it was working with third party cybersecurity experts and law enforcement to monitor the internet to assist in determining that the information relating to this incident was destroyed. At that time, it identified the vulnerability associated with this incident and quickly implemented a security fix. Blackbaud confirmed through testing by multiple third parties that their fix was able to withstand all currently known cyberattacks. As part of its ongoing cybersecurity efforts to help prevent an incident like this in the future, Blackbaud has implemented additional safety protocols to help protect data. Blackbaud is now offering the affected individuals credit monitoring as a result of discovering the extended impact of this incident.

WELS will notify the affected individuals and encourage them to activate the 24-months of free credit monitoring provided by Blackbaud. WELS is in the process of preparing the notices, which it will deliver in the most expedient time possible and without unreasonable delay.

Attached is a copy of the notification letter that WELS will place in the U.S. Mail Monday, November 9, 2020 to the affected individuals. There was no delay in providing individual notification as a result of law enforcement investigation. Please let us know if you have any questions or would like to discuss further.

If you have any questions, please do not hesitate to contact me.

Regards,



Adrienne S. Ehrhardt
Partner

Enclosure

[Letterhead]

<<FirstName>> <<LastName>>

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

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

Notice of Data Breach

Dear << FirstName>>:

We are writing to inform you about an update we received relating to a data security incident that occurred at Blackbaud, one of our third-party service providers, that may have involved your personal information. The Wisconsin Evangelical Lutheran Synod (“WELS”) operates Martin Luther College, the Michigan Lutheran Seminary, and the Wisconsin Lutheran Seminary (collectively, the “Educational Institutions”), and we engage Blackbaud for various services to help manage our donations and constituent communications and other services that help our Educational Institutions manage their student information.

WELS and our Educational Institutions take the protection and proper use of your information very seriously. We are therefore contacting you to notify you about the incident and provide you with steps you can take to protect yourself.

What Happened

On July 16, 2020, Blackbaud notified us that it suffered a ransomware attack in May 2020, which it successfully stopped with the help of independent forensics experts and law enforcement. We responded by taking appropriate action and notifying impacted individuals. At that time, Blackbaud assured WELS that the security incident was limited in scope and did not involve sensitive information such as Social Security Number. On or about September 29, 2020, however, Blackbaud notified WELS that it discovered that the incident impacted old unused tables from legacy services that neither WELS nor our Educational Institutions use any longer containing sensitive unencrypted information relating to WELS and our Educational Institutions. Blackbaud acknowledged that WELS and our Educational Institutions had no knowledge of the existence of these old tables.

What Information Was Involved

Blackbaud now informs us that the personal information that may have been accessed may include your name, date of birth, financial account number, and Social Security Number.

What Our Third-Party Provider is Doing

Blackbaud explained in its initial notice to WELS that it was working with third party cybersecurity experts and law enforcement to monitor the internet to assist in determining that the information relating to this incident was destroyed. At that time, it identified the vulnerability associated with this incident and quickly implemented a security fix. Blackbaud confirmed through testing by multiple third parties that their fix was able to withstand all currently known cyberattacks. As part of its ongoing cybersecurity efforts to help prevent an incident like this in the future, Blackbaud has implemented additional safety protocols to help protect data. Blackbaud is now offering you credit monitoring as a result of discovering the extended impact of this incident. The instructions are enclosed.

What We Are Doing

We are notifying you of this incident and will keep you updated with additional material information if it becomes available. We will continue to work with Blackbaud to further understand this incident and the steps they are taking to secure our data, as well as to understand why Blackbaud maintained outdated information for WELS and our Educational Institutions without our knowledge. We recommend you engage

[Letterhead]

the credit monitoring services provided by Blackbaud. Ensuring the safety of our constituents' and students' data is of the utmost importance to us. There was no delay in providing you this notification as a result of law enforcement investigation.

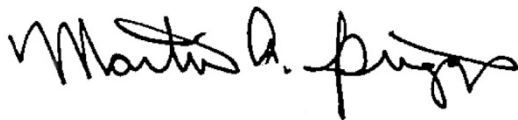
What You Can Do

In addition, we are providing you with the enclosed information about Identity Theft Protection which contains helpful information and resources. As a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. You should also regularly review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. If you see something you do not recognize, immediately notify your financial institution.

For More Information

We take the security and privacy of your information very seriously and apologize for any inconvenience this incident may have caused. Should you have any further questions or concerns regarding this matter, please contact dpo@wels.net or call us at [toll free number].

Sincerely,

A handwritten signature in black ink, appearing to read "Martin A. Spriggs". The signature is fluid and cursive, with the first name being the most prominent.

Martin A. Spriggs
WELS Chief Technology Officer
Data Protection Officer

How to Enroll in Credit Monitoring

We (Blackbaud) are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access to remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

Proactive Fraud Assistance

For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Identity Theft and Fraud Resolution Services

Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Enrollment Instruction

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to:

<https://www.cyberscouthq.com/epiq263?ac=263HQ1943>

If prompted, please provide the following unique code to gain access to services:

XXXXXXXXXX

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Information about Identity Theft Protection

Review Accounts and Credit Reports: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

Security Freezes and Fraud Alerts:

You have a 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. There is no fee for a security freeze. 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports at no charge. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and an incident report or complaint with a law enforcement agency or the Department of Motor

Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity; and
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, <https://www.consumerfinance.gov/learnmore/>, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

<p>Equifax (www.equifax.com)</p> <p>General Contact: P.O. Box 740241 Atlanta, GA 30374 800-685-1111</p> <p>Fraud Alerts: P.O. Box 740256 Atlanta, GA 30374</p> <p>Credit Freezes: P.O. Box 105788 Atlanta, GA 30348</p>	<p>Experian (www.experian.com)</p> <p>General Contact: P.O. Box 2002 Allen, TX 75013 888-397-3742</p> <p>Fraud Alerts and Security Freezes: P.O. Box 9554 Allen, TX 75013</p>	<p>TransUnion (www.transunion.com)</p> <p>General Contact, Fraud Alerts and Security Freezes: P.O. Box 2000 Chester, PA 19022 888-909-8872</p>
---	---	---