

Via Electronic Mail

securitybreach@atg.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 (“WELS”) to notify you of a recent security incident at Blackbaud, one of WELS’s service providers, that affected the personal information of some Washington state residents. WELS provides administrative, communication, financial, and other services to its members and congregations, supports mission work, and operates Lutheran schools, among other things. WELS engages Blackbaud for various services to help manage its donations and its donor information.

On or about July 16, 2020, Blackbaud notified WELS that it suffered a ransomware attack in May 2020, which it successfully stopped with the help of independent forensics experts and law enforcement. Unfortunately, the perpetrator was able to copy backups that contained data from WELS and many other nonprofits, schools, and colleges. Blackbaud did, however, pay the requested ransom to help ensure the backup file was permanently destroyed.

Blackbaud encrypts sensitive personal information such as Social Security Numbers, credit card numbers, and financial account information on its system. So, no such personal information was involved in this incident. The personal information that may have been impacted, however, includes name, address, telephone number, date of birth, and information relating to an individual’s relationship with WELS such as philanthropic giving history. This incident involved 772 Washington State residents. Blackbaud has informed us that there is no reason to believe that any data went beyond the cybercriminal; was or will be misused; or will be disseminated or otherwise made available publicly.

Blackbaud has informed WELS that it is 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. Blackbaud assured WELS that it identified the vulnerability associated with this incident, quickly implemented a security fix, and that it has implemented additional safety protocols that will help to protect WELS’ data. Additionally, Blackbaud is accelerating efforts to enhance access management, backups, encryption, network segmentation, deployment of additional endpoint and network-based platforms. WELS has notified the 772 Washington State residents. A copy of the notification letter that was mailed or emailed is attached.



August 10, 2020
Page 2

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

Regards,

Adrienne S. Ehrhardt
Adrienne S. Ehrhardt
Partner

August 4, 2020

Re: Notice of Data Breach

Dear [Name],

We are writing to inform you about 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”) engages Blackbaud for various services to help manage our donations and constituent communications. Blackbaud recently informed us that it experienced a data breach. WELS takes the security of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened

On or about 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. Unfortunately, the perpetrator was able to copy backups that contained data from WELS and many other nonprofits, schools, and colleges. Blackbaud, with the help of forensics experts and law enforcement, took the appropriate steps to help ensure the backup file was permanently destroyed.

What Information Was Involved

The personal information that may have been accessed included your name, address, telephone number, date of birth, and information relating to your relationship with WELS such as your philanthropic giving history. No sensitive information such as your Social Security Numbers, credit card numbers, or financial account information was accessed because that information is encrypted on Blackbaud’s systems. Blackbaud has informed us that there is no reason to believe that any data went beyond the cybercriminal; was or will be misused; or will be disseminated or otherwise made available publicly.

What Our Third-Party Provider is Doing

Blackbaud is 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. It identified the vulnerability associated with this incident and quickly implemented a security fix. As part of its ongoing efforts to help prevent an incident like this in the future, Blackbaud has implemented additional safety protocols that will help to protect your data. Additionally, Blackbaud is accelerating efforts to enhance access management, backups, encryption, network segmentation, deployment of additional endpoint and network-based platforms.

What WELS is Doing

While it appears that no sensitive personal information was accessed, out of an abundance of caution, 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

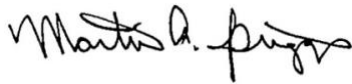
steps they are taking to secure our data. Ensuring the safety of our constituents' data is of the utmost importance to us.

What You Can Do

In addition, we are providing you with the enclosed information about Identity Theft Protection. Although Social Security numbers and other sensitive personal information were not at risk in this incident, 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.

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.

Sincerely,

A handwritten signature in black ink, appearing to read "Martin A. Spriggs". The signature is fluid and cursive, with a checkmark-like flourish at the beginning.

Martin A. Spriggs
WELS Chief Technology Officer
Data Protection Officer

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.

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. 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.

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) 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) 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) General Contact, Fraud Alerts and Security Freezes: P.O. Box 2000 Chester, PA 19022 888-909-8872</p>
--	--	--

