

NOTICE OF DATA BREACH:

What Happened? In October of 2018, Bayside Covenant Church, Inc. (“Bayside”) became aware of suspicious activity in certain employees’ email accounts. Bayside immediately began an investigation to confirm the nature and scope of this activity. Through the investigation, which included working with third party forensic investigators, we determined that the unauthorized actors accessed certain employees’ accounts without authorization between August 3, 2018 and October 20, 2018. Unfortunately, the investigation was unable to determine which emails or attachments may have been viewed without authorization. In an abundance of caution, the entire contents of the email accounts involved were reviewed to identify any personal information contained within the accounts. On December 19, 2018, the programmatic and manual review was completed, and it was determined that certain personal information was contained within the accounts that were accessed without authorization. To date, we have no information that there has been any actual or attempted misuse of the personal information within the accounts related to this event.

What Information Was Involved? The investigation in this matter confirmed that the following types of personal information were contained in the email accounts affected by this event included a combination of: name, address, date of birth, Social Security number, state identification number, driver’s license number, medical treatment and history, medical record and patient number, health insurance and benefit information, and financial account information

What We Are Doing? Bayside takes the confidentiality, privacy, and security of information in our care seriously and it is one of our highest priorities. Upon learning of the suspicious activity in the affected email accounts, we immediately commenced an investigation to confirm the nature and scope of the event. We took steps to identify the personal information contained in the affected email accounts and are notifying potentially impacted individuals of the event. As an added precaution, we are offering those individuals affected by the event access to credit monitoring, fraud consultation and identity theft repair services at no cost. Bayside is also notifying relevant regulators of the event as well.

While we have measures in place to protect information in our care, we are reviewing our existing policies and procedures following this event as part of our ongoing commitment to information security.

What You Can Do. We encourage you to please review the enclosed “Steps You Can Take to Protect Your Information,” which contains information on what you can do to better protect against possible misuse of your information, as well as information on the credit monitoring, fraud consultation and identity theft protection services we are offering and instructions on how to enroll. While we have no information that there has been misuse or attempted misuse regarding your information, including your account’s username or password, we encourage you to promptly change the credentials necessary for online accounts that use passwords.

Bayside encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com

or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-888-909-8872

www.transunion.com/cr/edi-freeze

Equifax

PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/cr/edit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289

www.transunion.com/fraud-victim-

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

[resource/place-fraud-alert](#)

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For Massachusetts residents, Under Massachusetts law, you have the right to obtain any 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. You can also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement, the FTC, and the Massachusetts Attorney General.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Rhode Island residents, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov.

For More Information. Bayside has set up a dedicated call center to answer questions from those who might be impacted by this event. The call center can be reached at 1-877-571-1215, Monday

through Friday 6:00 a.m. to 3:30 p.m., Pacific Time. If you do not receive a letter in the coming weeks, but want to confirm whether you are affected, please contact the call center at the number listed above.