

# **EXHIBIT 1**

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Bayside Covenant Church, Inc. (“Bayside”) does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data event notification statute, or personal jurisdiction.

### **Nature of the Data Event**

In October of 2018, 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. Third party forensic investigators were retained to assist with the investigation. Through these efforts, it was determined that unauthorized actors accessed certain employees’ accounts without authorization between August 3, 2018 and October 20, 2018. 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. Bayside then began a review of its files to locate address information for those individuals whose address information was not contained within the accessible emails.

The information that that was accessible within the email accounts includes name, address, Social Security Number, passport number, driver’s license number, financial account information, medical information, health insurance information, username and password for online account, and email and password.

### **Notice to California Residents**

On or about February 5, 2019, Bayside provided written notice of this incident to affected individuals, which includes one thousand, six hundred and eleven (1,611) California residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. Bayside is also notifying statewide media in California and posting notice of this even to its website, [www.baysideonline.com](http://www.baysideonline.com). A copy of the press release is attached here as *Exhibit B* and a copy of the web posting is attached here as *Exhibit C*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, Bayside moved quickly to investigate and respond to the incident, assess the security of Bayside systems, and notify potentially affected individuals. Bayside is also working to implement additional safeguards and training to its employees. Bayside is providing access to credit monitoring services at no cost for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident.

Additionally, while there is no evidence of individuals’ personal information being used or misused, Bayside is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Bayside is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details

for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

# **EXHIBIT A**



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

<<FirstName>> <<MiddleName>> <<LastName>> << NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

**Re: Notice of Data Breach**

Dear <<FirstName>> <<LastName>>,

Bayside Covenant Church, Inc. ("Bayside") writes to inform you of an incident that may impact the privacy of some of your personal information and to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

**What Happened?** In October of 2018, 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?** Our review identified the following information related to you that was contained within the email accounts: <<ClientDef1>><<ClientDef2 [data elements]>>.

**What We Are Doing?** The confidentiality, privacy, and security of information in our care is one of our highest priorities. 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.

As an added precaution, we are offering you access to twelve (12) months of credit monitoring, Fraud Consultation and Identity Theft Restoration through Kroll at no cost to you. We encourage you to enroll in these services as we are unable to enroll on your behalf.

**What You Can Do.** 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 restoration services we are offering and instructions on how to enroll.

**For More information.** We understand you may have questions that are not answered in this letter. If you have questions, please contact our dedicated call center at 1-877-571-1215 between 6:00 am and 3:30 pm Pacific Time, Monday through Friday.

Sincerely,

A handwritten signature in cursive script that reads "Nancy Short".

Nancy Short  
Bayside Covenant Church, Inc.

## STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

### **Enroll in Identity Monitoring**

While, to date, the investigation found no evidence that data potentially affected by this incident has been misused, in an abundance of caution, we are offering you access to identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Information on how to enroll in these services may be found below:

Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services.

*You have until May 2, 2019 to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-877-571-1215. Additional information describing your services is included with this letter.

### **Monitor Your Accounts**

We encourage 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 error over the next 12 to 24 months. 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](http://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**

PO Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 2000

Chester, PA 19016

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-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](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Additional Information**

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](http://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 and your state Attorney General. This notice has not been delayed by law enforcement.

**Take Advantage of Your Identity Monitoring Services**

You've been provided with access to the following services<sup>1</sup> from Kroll:

**Single Bureau Credit Monitoring.** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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)

<<FirstName>> <<MiddleName>> <<LastName>> << NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

## Re: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

Bayside Covenant Church, Inc. ("Bayside") writes to inform you of an incident that may impact the privacy of some of your personal information and to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

**What Happened?** In October of 2018, 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?** Our review identified the following information related to you that was contained within the email accounts: <<ClientDef1>><<ClientDef2 [data elements]>>.

**What We Are Doing?** The confidentiality, privacy, and security of information in our care is one of our highest priorities. 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.

As an added precaution, we are offering you access to twelve (12) months of credit monitoring, Fraud Consultation and Identity Theft Restoration through Kroll at no cost to you. We encourage you to enroll in these services as we are unable to enroll on your behalf.

**What You Can Do.** While we have no information that there has been misuse or attempted misuse regarding your account's username or password, we encourage you to promptly change the credentials necessary for online accounts that may use passwords. We also 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 restoration services we are offering and instructions on how to enroll.

**For More information.** We understand you may have questions that are not answered in this letter. If you have questions, please contact our dedicated call center at 1-877-571-1215 between 6:00 am and 3:30 pm Pacific Time, Monday through Friday.

Sincerely,

A handwritten signature in cursive script that reads "Nancy Short".

Nancy Short  
Bayside Covenant Church, Inc.



## STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

### **Enroll in Identity Monitoring**

While, to date, the investigation found no evidence that data potentially affected by this incident has been misused, in an abundance of caution, we are offering you access to identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Information on how to enroll in these services may be found below:

Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services.

*You have until May 2, 2019 to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-877-571-1215. Additional information describing your services is included with this letter.

### **Monitor Your Accounts**

We encourage 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 error over the next 12 to 24 months. 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](http://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**

PO Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 2000

Chester, PA 19016

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-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](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Additional Information**

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](http://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 and your state Attorney General. This notice has not been delayed by law enforcement.

**Take Advantage of Your Identity Monitoring Services**

You've been provided with access to the following services<sup>1</sup> from Kroll:

**Single Bureau Credit Monitoring.** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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)

Guardian

of

<<FirstName>> <<MiddleName>> <<LastName>> << NameSuffix>>

<<Address1>>

<<Address2>>

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

## Re: Notice of Data Breach

Dear Guardian of <<FirstName>> <<LastName>>,

Bayside Covenant Church, Inc. (“Bayside”) writes to make you aware of a recent incident that may affect the privacy of some of your minor dependent’s personal information. While there is currently no evidence that your minor dependent’s information has been misused, we are making you aware of the event, the steps we are taking in response, and steps you may take to better protect against possible misuse of your minor dependent’s personal information, should you feel it appropriate to do so.

**What Happened?** In October of 2018, 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?** Our review identified the following information related to your minor dependent that was contained within the email accounts: your minor dependent’s <<ClientDef1>><<ClientDef2 [data elements]>>.

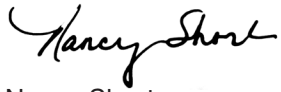
**What We Are Doing?** The confidentiality, privacy, and security of information in our care is one of our highest priorities. While we have measures in place to protect information in our care, we are reviewing our existing policies and procedures following this event as part of our ongoing commitment to information security.

While to date we have no evidence of misuse of your minor dependent’s information as a result of this event, as an added precaution, we are offering your minor dependent access to twelve (12) months of Fraud Consultation and Identity Theft Restoration through Kroll at no cost to you. We encourage you to enroll your minor dependent in these services as we are unable to enroll on your minor dependent on his or her behalf.

**What You Can Do.** 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 minor dependent’s information, as well as information on the credit monitoring, fraud consultation and identity theft restoration services we are offering and instructions on how to enroll.

**For More information.** We understand you may have questions that are not answered in this letter. If you have questions, please contact our dedicated call center at 1-877-571-1215 between 6:00 am and 3:30 pm Pacific Time, Monday through Friday.

Sincerely,

A handwritten signature in black ink that reads "Nancy Short". The signature is written in a cursive, flowing style.

Nancy Short  
Bayside Covenant Church, Inc.

## STEPS YOU CAN TAKE TO PROTECT YOUR MINOR DEPENDENT'S INFORMATION

### Kroll Fraud Consultation and Identity Theft Restoration

While, to date, the investigation found no evidence that data potentially affected by this incident has been misused, in an abundance of caution, we are offering you access to Fraud Consultation and Identity Theft Restoration at no cost to you for one year through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your child's Membership Number is: <<Member ID>>

Additional information describing your child's services is included with this letter.

### Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's dependent's account statements and credit reports, if such exist, for suspicious activity. Typically, a minor under the age of eighteen does not have credit in his or her name, and the consumer reporting agencies do not have a credit report in a minor's name; however, below are steps an individual can take to better protect his or her personal information, if a credit report has been issued in the individual's name:

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**

PO Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 2000

Chester, PA 19016

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-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](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000

Chester, PA 19106

1-800-680-7289

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

### **Additional Information**

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](http://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 and your state Attorney General. This notice has not been delayed by law enforcement.

### **Take Advantage of Fraud Consultation and Identity Theft Restoration Services**

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

**Fraud Consultation.** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your minor dependent's 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 your minor dependent becomes a victim of identity theft, an experienced Kroll licensed investigator will work on their behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your minor dependent's investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

# **EXHIBIT B**

## ***BAYSIDE COVENANT CHURCH PROVIDES NOTICE OF DATA BREACH***

***Bayside Covenant Church, Inc. (02/05/19)***

***What Happened?*** In October of 2018, 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, Social Security Number, passport number, driver's license number, financial account information, medical information, health insurance information, username and password for online account, and email and password.

***What We Are Doing?*** Bayside takes the confidentiality, privacy, and security of information in our care is 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.*** Bayside encourages potentially impacted individuals 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 residents are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Affected individuals may also contact the three major credit bureaus directly to request a free copy of your credit report.

Affected individuals have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without their express authorization. The security freeze is designed to prevent credit, loans, and services from



being approved in the individual's name without his or her consent. However, affected individuals should be aware that using a security freeze to take control over who gets access to the personal and financial information in their 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, affected individuals cannot be charged to place or lift a security freeze on their credit report. Should affected individuals 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](http://www.experian.com/freeze/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/cr/edi-freeze](http://www.transunion.com/cr/edi-freeze)

**Equifax**

PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, affected individuals 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, affected individuals have the right to place an initial or extended "fraud alert" on their 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 an affected individual is a victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should affected individuals 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](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

Affected individuals can further educate themselves 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](http://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. Affected individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Affected individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, affected individuals will likely need to provide some proof that they 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.

While we have no information that there has been misuse or attempted misuse of the personal information accessible, Bayside encourages affected individuals to promptly change passwords for any account that may share a password.

***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. Additional information can also be found at the Bayside's website, <https://www.baysideonline.com/>.

# **EXHIBIT C**

## ***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](http://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](http://www.experian.com/freeze/center.html)

**TransUnion**

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

[www.transunion.com/cr/edi-freeze](http://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](http://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

**TransUnion**

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

**Equifax**

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

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

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](http://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, 16<sup>th</sup> Floor, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://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](http://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](http://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](http://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.