LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

SIAN SCHAFLE
DIRECT DIAL: 215.977.4067
SIAN.SCHAFLE@LEWISBRISBOIS.COM

June 21, 2016

VIA E-MAIL AND U.S. MAIL
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: idtheft@oag.state.md.us

Re: **Notice of Data Event**

Dear Sir or Madam:

We represent National Church Solutions, 2670 Pyramus Road, Chester, WV 26034 ("NCS") and are writing to notify your office of an incident that affects the security of personal information relating to one (1) Maryland resident organization. By providing this voluntary notice, NCS does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Nature of Data Event

On or about February 8, 2016, the Federal Bureau of Investigation ("FBI") informed NCS that it had detected a malicious IP address communicating with its network. NCS immediately launched an internal investigation and began working with a third-party forensic company assist in the investigation into the suspicious communication with its network.

On May 5, 2016 NCS determined that a virus infected certain devices on its systems between February 3, 2016 and February 9, 2016, and that this virus may have resulted in unauthorized access to some information related to certain businesses with which it works, including the organization's: address, phone number, bank account information and the Federal Tax Identification number. This virus may have also permitted unauthorized access to certain information relating to certain individuals, such as an individual's name, address, date of birth and Social Security number.

Notice to Organization Operating In Maryland

On June 21, 2016, NCS will begin notifying organizations whose information may have been accessed during this incident, which includes one (1) organization operating in Maryland. This notice will provide details of the incident, information on steps the organization can take to protect the its information, and contact information the organization may use should it have questions or concerns. The notice letter that will

be provided to affected organizations is in substantially the same form as the letter attached here as ***Exhibit A***. On that same date, NCS will begin providing notice of this incident to those individuals whose personal information may have been accessed during this incident. There were no Maryland residents impacted by this incident.

Other Steps Taken and To Be Taken

Upon discovering this incident, NCS moved quickly to identify whether the virus may have accessed information stored within its network, determine whose information may have been accessed and confirm that the virus was no longer accessing its network or information stored thereon. Additionally, NCS is providing potentially affected individuals and organizations with information on how to better protect against misuse of the organization's information, including information on how to place a fraud alert and security freeze on the organization's credit file, information on and encouragement to contact the Federal Trade Commission, state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 215-977-4067.

Very truly yours,

Sian M. Schafle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

SMS:ncl
Enclosure

EXHIBIT A

[Organization Name]
[Street Address]
[City, State Zip Code]

RE: Notice of Data Incident

Dear [Organization Name]:

National Church Solutions recently discovered an incident that may affect the security of your organization's information. We write to provide you with information about the incident, steps taken since discovering the incident, and information on what you can do to better protect your organization's information.

What Happened? On or about February 8, 2016, the Federal Bureau of Investigation ("FBI") informed us they had detected a malicious IP address communicating with our network. We immediately launched an internal investigation and retained a third-party forensic investigation firm to assist in the investigation of the incident.

What Information Was Involved? Utilizing third-party forensic investigation firm, on May 5, 2016 we determined that a virus infected certain devices on our systems between February 3, 2016 and February 9, 2016, and that this virus may have resulted in unauthorized access to information about your organization, including [data elements].

What We Are Doing. We take this incident and the security of our clients' information very seriously. We have stringent security measures in place to safeguard the information in our possession. As a result of this incident, we are working to implement additional safeguards to protect the privacy and security of information on our systems.

For More Information. Call the call center we've established regarding this incident. The call center is staffed with professionals who can answer questions about this incident and give you information on how to protect against misuse of your information. The call center is available Monday through Friday, 9:00 AM until 9:00 PM EDT and Saturday through Sunday, 11:00 AM until 8 PM EDT at 866-751-1324.

We take the privacy of your personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you. The security of your information is a priority to us and we have taken precautionary measures to mitigate the risk of any future reoccurrence.

We sincerely apologize for any inconvenience or concern this may have caused.

Sincerely,

[Name]
[Title]

DRAFT

OTHER IMPORTANT INFORMATION

You may take action directly to further protect against possible identity theft or financial loss, both as an individual and as an organization. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

You can also place a "security freeze" on your credit file that prohibits a credit reporting agency from releasing any information from your credit report without your written authorization but may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift or remove a security freeze. In all other cases, a credit agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You must contact each of the credit reporting agencies separately to place a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion LLC
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3742	888-909-8872
800-349-9960 (NY Residents)		
http://www.freeze.equifax.com	www.experian.com	freeze.transunion.com

You can further educate yourself further on identity theft, fraud alerts, and the steps one can take to protect against identity theft and fraud by contacting 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. For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. In addition, we recommend reporting suspicious activity or incidents of identity theft and fraud to local law enforcement.

DRAFT