

EXHIBIT 1

The investigation into this matter has completed and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, College Church does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

College Church became aware of suspicious activity related to their email environment. College Church promptly launched an investigation, with the assistance of third-party specialists, to determine the nature and scope of the activity. The investigation determined that there was unauthorized access to a College Church email account from November 14, 2024, through January 21, 2025. Thereafter, College Church undertook a comprehensive review of the data at risk associated with the potentially impacted email account to assess if any sensitive information could be affected and to whom it relates. College Church then worked to identify appropriate contact information for the potentially impacted individuals. College Church completed their address enrichment process on November 26, 2025, at which point they promptly moved to provide notice to individuals that may have been impacted by the event.

The information that could have been subject to unauthorized access includes name and driver's license number.

Notice to Nebraska Residents

On or about December 22, 2025, College Church provided written notice of this incident to one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, College Church moved quickly to investigate and respond to the incident, assess the security of College Church systems, and identify potentially affected individuals. College Church is also working to implement additional safeguards and training to its employees. College Church is providing access to credit monitoring services for twelve (12) months, through Cyberscout, a TransUnion company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, College Church is providing impacted individuals with guidance on how to better protect against identity theft and fraud. College Church 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.

College Church is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A



0000056

College Church
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2474



3_0000056



[REDACTED]

[REDACTED]

Wheaton, IL 60187-3009



December 22, 2025

NOTICE OF SECURITY INCIDENT

Dear [REDACTED]y:

College Church writes to inform you of an incident that may impact the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to help protect your information should you feel it is appropriate to do so.

What Happened? College Church became aware of suspicious activity related to their email environment. College Church promptly launched an investigation, with the assistance of third-party specialists, to determine the nature and scope of the activity. The investigation determined that there was unauthorized access to a College Church email account from November 14, 2024 through January 21, 2025. Thereafter, College Church undertook a comprehensive review of the data at risk associated with the potentially impacted email account to assess if any sensitive information could be affected and to whom it relates. College Church then worked to identify appropriate contact information for the potentially impacted individuals. College Church completed their address enrichment process on November 26, 2025, at which point they promptly moved to provide notice to individuals that may have been impacted by the event.

What Information Was Involved? The following information related to you could have been affected: name, health insurance information, Social Security number, payment card information, driver or state license number, medical information, and financial account information.

What We Are Doing. The confidentiality, privacy, and security of information within our care are among College Church's highest priorities. Upon learning of the incident, we commenced an investigation to understand the nature and scope of the incident. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies, and procedures related to data privacy and security to reduce the likelihood of a similar future incident.

As an added precaution, we are offering you access to twelve (12) months of complimentary credit monitoring and identity restoration services through Cyberscout, a TransUnion company. Individuals who wish to receive these services can enroll by following the enrollment instructions as we are unable to activate the services on your behalf.

Enroll in Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with

alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud. You can review the enclosed *Steps You Can Take To Help Protect Your Information* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions, or need assistance, please call our dedicated assistance line at 1-800-405-6108 Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time. You may also write to College Church, 332 East Seminary Avenue, Wheaton, IL 60187 or email us at incident@college-church.org.

Sincerely,

College Church

Steps You Can Take To Help Protect Your Information



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, they may contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit 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 they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, they should contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further

information on how to file such a complaint by way of the contact information listed above. Consumers 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, consumers 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 and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There is approximately 1 Rhode Island resident that may be impacted by this event.