

EXHIBIT 1

We represent First Baptist Church of Hammond (“FBC Hammond”) located at 507 State Street, Hammond, IN 46320, and write to notify your office of a matter that may affect the security of certain information relating to approximately eight (8) Nebraska residents. By providing this notice, FBC Hammond 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

On July 5, 2025, FBC Hammond identified connectivity issues on certain computer systems on the computer network. FBC Hammond subsequently learned on July 7 that an unknown cyber actor accessed its computer network and used a virus to lock files on certain computer systems. After this issue was identified, FBC Hammond took steps to confirm the security of the computer network and determine what occurred. While the investigation was ongoing, FBC Hammond published a notice on its website on July 15 to keep the community informed of its response to and review of this matter. The review of this matter later determined that files were copied from the computer network between June 29 and July 2, 2025. After identifying the files involved, FBC Hammond located the files to review them. This review was necessary to identify and notify individuals about this matter. The file review was complete on August 7, 2025, and identified that the following type(s) of information were in the reviewed files name(s), Social Security number, and driver’s license number. After completing the review, FBC Hammond arranged services to provide individuals with notice and an offer of complimentary identity monitoring.

Notice to Nebraska Residents

On August 21, 2025, FBC Hammond provided written notice of this matter to approximately eight (8) Nebraska residents. 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 identifying this matter, FBC Hammond moved quickly to investigate what occurred, assess the security of its systems, and identify potentially affected individuals. Further, First Baptist notified federal law enforcement regarding the event. FBC Hammond has safeguards in place to protect information in its care, and as part of its response to this matter it implemented supplemental controls and practices to reduce the risk of an event like this reoccurring. FBC Hammond is also providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, FBC Hammond is providing notified individuals with guidance on how to better protect against identity theft and fraud. FBC Hammond 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



First Baptist Church of Hammond
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1640

20_0005087



August 21, 2025

Notice of Data Breach

Dear [REDACTED]:

First Baptist Church of Hammond and Its Ministries writes to notify you about a matter that involves your information. This letter provides you with information about what happened, our response, and steps you may take should you feel it is appropriate.

What Happened? On July 5, 2025, we identified connectivity issues on certain computer systems on the computer network. We subsequently learned on July 7 that an unknown cyber actor accessed our computer network and used a virus to lock files on certain computer systems. After this issue was identified, we took steps to confirm the security of the computer network and determine what occurred. While the investigation was ongoing, we published a notice on our website on July 15 to keep the community informed of our response to and review of this matter. Our review of this matter later determined that files were copied from the computer network between June 29 and July 2, 2025. After identifying the files involved, we located the files to review them. This review was necessary for us to identify and notify individuals about this matter. The file review was complete on August 7, 2025, which allowed us to arrange services to provide individuals with notice and an offer of complimentary identity monitoring.

What Information Was Involved? The copied files contained your name and Social Security number.

What We Are Doing. Following our review, we are notifying individuals to ensure they are aware of this matter. Additionally, we are providing individuals with free resources and guidance, including identity monitoring services. While no safeguards can fully prevent all cybersecurity matters, we have taken measures to reduce the risk of an issue like this reoccurring. We will continue to evaluate and update our policies and practices as appropriate.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the "Steps Individuals Can Take To Protect Personal Information" section of this letter. Further, you may enroll in the complimentary identity monitoring services. The enrollment instructions can be found in the "Enroll in Monitoring Services" section of this letter. Please note that, due to privacy restrictions, we are unable to automatically enroll you in the complimentary identity monitoring services.

For More Information. If you have questions about this matter, we have an assistance line with agents ready to help answer your questions. Please contact our toll-free assistance line at 1-833-426-8015, Monday through Friday, from 8:00 a.m. to 8:00 p.m. Eastern Time Eastern Time (excluding U.S. holidays). You may also write to us at First Baptist Church of Hammond, Attn: Compliance, 507 State Street Hammond, IN 46320.

Sincerely,

First Baptist Church of Hammond

Steps Individuals Can Take To Protect Personal Information

Enroll in Monitoring Services

In response to the matter, 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 the 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.

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.

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, please 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, please 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/>. First Baptist Church of Hammond, Attn: Compliance, 507 State Street Hammond, IN 46320 or 1-219-932-0711.

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 Avenue NW, 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 contacted 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 are approximately 2 Rhode Island residents that may be impacted by this event.