Notice of Data Event

Updated July 15, 2025

First Baptist Church of Hammond and Its Ministries writes to update the community about a cyber event involving files stored on our computer network. This notice provides information about what happened, our response, and steps individuals may take should they feel it is appropriate to do so. To ensure our community is provided with up-to-date, accurate information about this matter, our website will be the primary method of sharing information. The community is encouraged to check our website for updates, and to understand that our staff will refer individuals inquiring about this matter to our website. Our website will remain the central source of information about this matter.

What Happened? In July 2025, an unknown cyber actor accessed our computer network and used a virus to lock files stored on certain computer systems. In response, the computer network was taken offline to review what happened and to begin secure recovery efforts. The investigation into this matter is ongoing as of this update, and we do not have full details on what has occurred and how this impacts data stored on the computer network. Technical investigations are complex and take time to complete. We do not have an estimated date for completion at this time. The investigative challenges are also exacerbated by the computer virus locking the computers that contain evidence. We continue to ask the community for their patience and respect for the integrity of the investigative process.

What Information Was Involved? Although the investigation remains in its earliest stages, we have learned that files containing information for staff and missionaries were copied. The files contain individuals' government identifiers, including Social Security, driver's license and passport numbers. With respect to some self-funded health plan participants, the data involved will vary by participant but collectively includes name, address, contact information, unique healthcare identifier, date of birth, and/or health information for self-funded health plan claims processing. We will continue to update this section should we learn additional groups of individuals' information was involved, including volunteers.

Does This Impact Congregation Member Information? We do not typically store personal information for congregation members, unless those members are also staff, missionaries or volunteers.

What We Are Doing. We are providing guidance in the "Steps Individuals Can Take To Protect Personal Information" section below. Further, we are also examining additional resources to help individuals with monitoring and protecting their personal information. Additionally, while we do have safeguards in place to protect information in our care, as part of our response to this matter, we will evaluate supplemental technical security measures and practices to reduce the risk of an event like this reoccurring.

What Individuals Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity and to detect errors. We also encourage individuals to review the below "Steps Individuals Can Take To Protect Personal Information" section. This section contains free resources that are available, including guidance for monitoring free credit reports, how to place a fraud alert or security freeze on credit files, and contact information for the consumer reporting agencies and Federal Trade Commission.

For More Information? To best assist individuals, we will establish a toll-free assistance line to answer questions about this matter. In the interim, should individuals have any concerns about this matter, they may review the free resources and guidance below. Individuals 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 and Its Ministries

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Relevant 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—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

For loved ones that may have recently passed, individuals may also place a "deceased – do not issue credit" flag on the loved one's credit file. Only one consumer reporting bureau needs to be notified, and it will notify the other two major consumer reporting bureaus. Individuals may complete this process using the information provided by the credit bureaus at the below websites:

Equifax: https://www.equifax.com/personal/help/article-list/-/h/a/relative-death-contact-credit-bureaus
Experian: https://www.experian.com/blogs/ask-experian/reporting-death-of-relative/
TransUnion: https://www.transunion.com/blog/credit-advice/reporting-a-death-to-tu

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, DC 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.

STEPS INDIVIDUALS CAN TAKE TO PROTECT THEIR MINOR DEPENDENTS' PERSONAL INFORMATION

Monitor Relevant Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor dependent has a credit report or to request a manual search for your minor dependent's Social Security number, each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit or contact the below credit bureaus.

Equifax—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

To request information about the existence of a credit file in your minor dependent's name, search for your dependent's Social Security number, place a security freeze on your dependent's credit file, place a fraud alert on your dependent's credit report (if one exists), or request a copy of your dependent's credit report you may be required to provide some or all the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor dependent's birth certificate;
- A copy of your minor dependent's Social Security card;
- Your minor dependent's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor dependent's date of birth; and
- Your minor dependent's previous addresses for the past two years.

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps individuals can take to protect 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, DC 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. A parent and/or their minor dependent have the right to file a police report if the minor dependent ever experiences identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, the parent or the minor dependent will likely need to provide some proof that the minor dependent has been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state Attorney General.