EXHIBIT 1

By providing this notice, FBCG 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 or around October 31, 2024, FBCG detected suspicious activity related to its network and began an investigation into the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to its network and acquired certain files between October 12, 2024, and October 28, 2024. FBCG then conducted a detailed review of the potentially impacted data to determine what information it may contain and to whom it belongs. Once this was recently completed, FBCG worked to obtain mailing addresses for impacted individuals to provide written notice. FBCG then worked to provide notification to impacted individuals.

The information that could have been impacted includes name, and Social Security number.

Notice to Nebraska Resident

On or about December 5, 2025, FBCG 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, FBCG moved quickly to investigate and respond to the incident, assess the security of FBCG systems, and identify potentially affected individuals. Further, FBCG notified federal law enforcement regarding the event. FBCG is providing access to credit monitoring services for one (1) year through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

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

FBCG is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

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

<<b2b_text_1 (variable header: NOTICE OF [SECURITY INCIDENT / DATA BREACH])>>

Dear <<First_name>> <<Middle_name>> <<Last_name>> <<Suffix>>:

First Baptist Church of Glenarden International ("FBCG") writes to inform you of an event that may impact the privacy of some of your personal information. We are providing you with information about the event, our response, and steps you may take to protect against any misuse of your information, should you feel it is necessary to do so.

What Happened? On or around October 31, 2024, FBCG detected suspicious activity related to our network and began an investigation into the nature and scope of the activity. Our investigation determined that an unauthorized actor gained access to our network and acquired certain files between October 12, 2024, and October 28, 2024. We then conducted a detailed review of the potentially impacted data to determine what information it may contain and to whom it belongs. This review was recently completed, which is when it was determined that your information was potentially impacted.

What Information Was Involved? The following type of information related to you may have been impacted: <<b2b_text_2 ("name", data elements)>>. FBCG is not aware of any actual or attempted misuse of your information in connection with this incident.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon discovering the suspicious activity, we immediately commenced an investigation to confirm its nature and scope. We also implemented additional security measures related to data privacy and security. As an added precaution, we are offering you access to credit monitoring and identity restoration assistance services for 12 months through Kroll at no cost to you. A description of services and instructions regarding how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. In addition to enrolling in the credit monitoring services being offered to you, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and reporting suspected identity theft and fraud to your credit card company or bank. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information.* There you will also find more information regarding ways to protect and monitor your information.

For More Information. If you have further questions or concerns, or would like an alternative to enrolling online, please call (844) 572-2715 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. You may also write to us at Business Services Department, 3600 Brightseat Road, Hyattsville, MD 20769.

Sincerely,

First Baptist Church of Glenarden

Steps You Can Take To Help Protect Personal Information

<u>Enroll in Monitoring Services</u>

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. 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.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: `<<Membership Number s_n>>`

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will be able to help you determine if it is an indicator of identity theft. 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.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

<u>Monitor Your Accounts</u>

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 your 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

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 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.