



Loree Stuck, Partner
Cybersecurity & Data Privacy Team
550 West C Street, Ste 1400
San Diego, CA 92101
lstuck@constangy.com
Telephone: 206.552.5069

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

March 23, 2026

VIA ONLINE SUBMISSION

Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notification of Data Security Event

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Chapel Hill Presbyterian Church (“Chapel Hill Church”), a Presbyterian church located in Gig Harbor, Washington, in connection with its response to a recent data security incident. The purpose of this letter is to notify you of the event in accordance with the Washington data breach notification statute. By providing this notice, Chapel Hill Church does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

1. Nature of the Security Event

On January 30, 2026, Chapel Hill Church became aware of unusual network activity and immediately took steps to secure our systems. Chapel Hill Church engaged cybersecurity experts to assist with the process. The investigation determined that certain Chapel Hill Church data may have been acquired without authorization on or about February 6, 2026. As a result, Chapel Hill Church undertook a comprehensive review of all potentially affected files to identify individuals whose information may have been involved and gather contact information necessary to effectuate notice. These efforts concluded on February 26, 2026, at which time Chapel Hill Church arranged to provide notice to all potentially affected individuals.

2. Number of Affected Washington Residents & Information Involved

The event involved personal information for approximately 879 Washington residents. The information potentially involved for identified Washington residents varied by individual and may have included name, date of birth, Social Security number, driver’s license number, and passport number.

3. Notification to Identified Individuals

On March 23, 2026, Chapel Hill Church mailed notification letters to identified Washington residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. A sample notification letter is enclosed.

4. Measures Taken to Address the Event

Upon identifying the suspicious activity, Chapel Hill Church launched an investigation to determine the nature and scope of the event, conducted a thorough and comprehensive review to determine what information was involved and to whom such information relates, and notified the identified individuals. The notification letters provide identified individuals with information regarding steps they can take to protect their personal information, including information about the toll-free call center established for answering questions about the event and addressing related concerns.

5. Contact Information

If you have any questions or need additional information regarding this event, please do not hesitate to contact me at lstuck@constangy.com.

Sincerely,

A handwritten signature in cursive script that reads "Loree Stuck".

Loree Stuck
Partner, Constangy Cyber Team



Return Mail Processing Center:
PO Box 173071 | Milwaukee, WI 53217

<<First Name>> << Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

Subject: Notice of Data <<Header>>

Dear <<First Name>> << Last Name>>:

We are writing to inform you about a recent data security incident experienced by Chapel Hill Presbyterian Church ("Chapel Hill Church") that may have involved your information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On January 30, 2026, Chapel Hill Church became aware of unusual activity within its digital environment that disrupted access to certain systems. Upon discovery, Chapel Hill Church immediately took steps to secure its network and engaged leading cybersecurity experts to investigate. As a result of the investigation, Chapel Hill Church learned that certain information was acquired without authorization by an unknown party. Chapel Hill Church then commenced a review of the affected data to determine whether any personal information may have been affected. Following a thorough review of the impacted data, on February 26, 2026, the review concluded, and Chapel Hill Church confirmed that your information was involved. We then took steps to notify you of the incident as quickly as possible.

Please note that Chapel Hill Church has no evidence of any actual or suspected misuse of information involved in this incident.

What Information Was Involved? The information that was potentially impacted during this incident included your name, as well as your <<Data Elements>>.

What Are We Doing? As soon as we discovered the incident, we took the steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation.

Additionally, although we have no indication at this time of any misuse of your information, we have secured the services of Iris Identity Protection to provide complimentary identity monitoring for <<CM Duration>> months at no charge. To enroll in the credit monitoring services at no charge, please visit <https://iris-pro.myidentityprotectiononline.com> and enter the following promo code to enroll and begin your membership: <<Monitoring Code>> (case sensitive). Please note the deadline to enroll is 90 days from the date of this letter. Iris Identity Monitoring provides One-bureau credit monitoring from Equifax®, Identity Monitoring, Identity Fraud Insurance¹, and Identity Resolution Services.

¹ The Identity Expense Reimbursement and the Unauthorized Electronic Fund Transfer Reimbursement benefits are underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Generali Global Assistance, Inc., dba Iris® Powered by Generali for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. Review the Summary of Benefits at <https://www.irisidentityprotection.com/terms-conditions>.

What Can You Do? We encourage you to enroll in the credit protection services we are offering, which are at no cost to you. Please also review the guidance at the end of this letter, which includes additional resources you may utilize to help protect your information.

For More Information: If you have questions or need assistance, please contact 877-507-2354 Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time, excluding major U.S. holidays. Representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Sincerely,

Chapel Hill Presbyterian Church

7700 Skansie Avenue
Gig Harbor, WA 98335

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>. The total number of Rhode Island residents receiving notification of this incident is zero.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov



Return Mail Processing Center:
PO Box 173071 | Milwaukee, WI 53217

<<First Name>> << Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

Subject: Notice of Data <<Header>>

Dear <<First Name>> << Last Name>>:

We are writing to inform you about a recent data security incident experienced by Chapel Hill Presbyterian Church (“Chapel Hill Church”) that may have involved your information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On January 30, 2026, Chapel Hill Church became aware of unusual activity within its digital environment that disrupted access to certain systems. Upon discovery, Chapel Hill Church immediately took steps to secure its network and engaged leading cybersecurity experts to investigate. As a result of the investigation, Chapel Hill Church learned that certain information was acquired without authorization by an unknown party. Chapel Hill Church then commenced a review of the affected data to determine whether any personal information may have been affected. Following a thorough review of the impacted data, on February 26, 2026, the review concluded, and Chapel Hill Church confirmed that your information was involved. We then took steps to notify you of the incident as quickly as possible.

Please note that Chapel Hill Church has no evidence of any actual or suspected misuse of information involved in this incident.

What Information Was Involved? The information that was potentially impacted during this incident included your name, as well as your <<Data Elements>>.

What Are We Doing? As soon as we discovered the incident, we took the steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation.

Additionally, although we have no indication at this time of any misuse of your information, we have secured the services of Iris Identity Protection to provide complimentary identity monitoring for <<CM Duration>> months at no charge. To enroll in the credit monitoring services at no charge, please visit <https://iris-pro.myidentityprotectiononline.com> and enter the following promo code to enroll and begin your membership: <<Monitoring Code>> (case sensitive). Please note the deadline to enroll is 90 days from the date of this letter. Iris Identity Monitoring provides One-bureau credit monitoring from Equifax®, Identity Monitoring, Identity Fraud Insurance¹, and Identity Resolution Services.

¹ The Identity Expense Reimbursement and the Unauthorized Electronic Fund Transfer Reimbursement benefits are underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Generali Global Assistance, Inc., dba Iris® Powered by Generali for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. Review the Summary of Benefits at <https://www.irisidentityprotection.com/terms-conditions>.

What Can You Do? We encourage you to enroll in the credit protection services we are offering, which are at no cost to you. Please also review the guidance at the end of this letter, which includes additional resources you may utilize to help protect your information.

For More Information: If you have questions or need assistance, please contact 877-507-2354 Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time, excluding major U.S. holidays. Representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Sincerely,

Chapel Hill Presbyterian Church

7700 Skansie Avenue
Gig Harbor, WA 98335

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>. The total number of Rhode Island residents receiving notification of this incident is zero.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov