



September 18, 2020

Via Email

Washington State Attorney General's Office
1125 Washington St SE
PO Box 40100
Olympia, WA 98504
Securitybreach@atg.wa.gov

Orrick, Herrington & Sutcliffe LLP
701 Fifth Avenue
Suite 5600
Seattle, WA 98104-7097
+1 206 839 4300
orrick.com

Aravind Swaminathan

E aswaminathan@orrick.com
D +1 206 839 4340
F +1 206 839 4301

RE: Notification of Data Security Event / St. Hubert Church

Dear Attorney General:

We are writing to inform you of a security incident that may have affected some of our parishioners. On August 20, 2020, a laptop computer owned by St. Hubert's Church was stolen from an employee's automobile. Law enforcement was promptly informed. Although the laptop was protected by certain security features and required a pin number to access it, the laptop's hard drive was not encrypted.

The laptop contained our parishioner tracking database, which includes information such as names of parishioners, contact information, and dates of birth. We identified personal information—dates of birth—for 657 Washington residents. We have no indication that this event resulted in any misuse of personal information.

We began notifying Washington State residents via letter on September 18, 2020, and we have attached a sample copy of the notification. We are offering one year of free credit monitoring services to those whose personal information was impacted.

If your office requires any further information in this matter, please contact me at (206) 839-4340 or aswaminathan@orrick.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Aravind Swaminathan".

Aravind Swaminathan

Partner

Global Co-Chair Cyber, Privacy & Data Innovation



ST. HUBERT
CATHOLIC CHURCH

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a security incident that may have affected some of our parishioners. On August 20, 2020, a laptop computer owned by St. Hubert's Church was stolen from an employee's automobile. Law enforcement was promptly informed. Although the laptop was protected by certain security features and required a pin number to access it, the laptop's hard drive was not encrypted.

What Information Was Involved

Our records indicate that this security incident may have affected some of your personal information. The laptop contained our parishioner tracking database, which includes information such as names of parishioners, contact information, and dates of birth. **The thief did NOT access credit card information or Social Security numbers**, since this information was not stored on this laptop. We have no indication that this event resulted in any misuse of your personal information but are notifying you so you can take certain precautions.

What We Are Doing

We take data security very seriously, especially as it relates to personal information. We deeply regret that this situation occurred and are offering you free credit monitoring, provided by Experian. Please refer to the credit monitoring section of this letter, Attachment A, for more information about these credit monitoring services and how to sign up.

What You Can Do

We encourage you to consider taking the following precautions:

- We urge you to remain vigilant against threats of identity theft or fraud. Regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. Report any unauthorized activity on your credit or banking accounts to your credit or banking providers immediately.
- Be alert for "phishing" emails from someone who acts like they know you and requests sensitive information over email, such as passwords, Social Security numbers or bank account information.
- It is always best practice to change your financial account passwords often.
- If you suspect you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement.
- You may contact the FTC or the Washington State Attorney General to learn more about protecting yourself against identity theft. Attachment B, titled "Additional Information to Protect Yourself," has more information about steps you can take to protect yourself against identity theft or fraud.

For More Information

For more information about this matter, or if you have additional questions or concerns, you may contact the church directly at pastoralasst@whidbey.com. Again, we sincerely regret any concern this matter may cause.

Sincerely,

Susan Walker
Pastoral Administrator, St. Hubert Church

Attachments

Attachment A

Credit Monitoring Services

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by:** <<b2b_text_1(EnrollmentDeadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** <<Member ID>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057 by <<b2b_text_1(EnrollmentDeadline)>>. Be prepared to provide engagement number <<b2b_text_2(EngagementNumber)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.288.8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment B

Additional Information to Protect Yourself

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 726-1014.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

Consider contacting the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit.

A security freeze prohibits a credit-reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

A credit-reporting agency may not charge you to place, temporarily lift or permanently remove a security freeze. To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax:
Consumer Fraud Division
P.O. Box 105069
Atlanta, GA 30348
(888) 836-6351
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion:
TransUnion LLC
P.O. Box 160
Woodlyn, PA 19094
(800) 909-8872
www.transunion.com

You may obtain information about preventing identity theft at atg.wa.gov/identity-theftprivacy. You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes and how to protect yourself from identity theft. The FTC can be contacted at 600 Pennsylvania Ave. NW, Washington, DC 20580; telephone (202) 326-2222; or www.consumer.gov/idtheft.