



July 14, 2025

Office of the Attorney General
Washington State
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

Via Electronic Submission

RE: PERSONAL DATA BREACH NOTIFICATION

To whom it may concern,

In accordance with RCW §§ 19.255.010(7) and 42.56.590(7)), we are submitting via the online portal at <https://fortress.wa.gov/atg/formhandler/ago/databreachnotificationform.aspx> information regarding a personal data breach, including template copies of the notifications sent today to affected residents of Washington.

Although the breach involved a single centralized database operated by BYU-Pathway Worldwide, the database included some BYU-Pathway students who have moved on to finish their degree with our partners BYU-Idaho and Ensign College. Affected individuals will receive notice on the letterhead of the institution with which they are currently affiliated—or most recently affiliated—at the time of the incident, but the notices are otherwise identical.

Our Global Privacy Officer is available to provide any further information that you may require and can be contacted at:

Denise Farnsworth
Global Privacy Officer
50 E. North Temple Street
Salt Lake City, Utah 84150
United States
Denise.Farnsworth@churchofjesuschrist.org
+1 801-353-2149

Yours faithfully,
L. Denise Farnsworth
Senior Counsel and Global Privacy Officer
Office of General Counsel
The Church of Jesus Christ of Latter-day Saints
50 E. North Temple Street
Salt Lake City, Utah 84150
United States
Denise.Farnsworth@churchofjesuschrist.org

NOTICE OF DATA BREACH

Dear student,

BYU-Pathway Worldwide, a Utah nonprofit corporation, recently detected unauthorized network access that may have included your personal data. At this time, there is no evidence that your personal information has been used for fraudulent or other harmful purposes. We are notifying you and others whose data may have been affected, even where this is not legally required.

What happened?

The BYU-Pathway information security team became aware of a potential security incident that occurred on or about 17 June 2025 involving a vendor's account. On 24 June 2025, after we became aware of the unauthorized access, we removed the vendor's access to any personal information. We then notified federal law enforcement authorities in the United States and engaged cybersecurity experts. Upon investigation, evidence indicated the vendor's account was compromised by an unknown third party, which allowed unauthorized access to certain systems.

Who committed this intrusion?

BYU-Pathway cannot determine the identity of the unauthorized person who may have accessed or acquired your personal data. The forensic investigators who assisted BYU-Pathway in investigating the security breach have not detected any further unauthorized access or activity since 24 June 2025.

What information was affected?

The personal information accessed may have included your name; Social Security number (if you provided it); your account ID (but not password); contact information, such as address and phone number; gender and marital status; religious affiliation (if you provided it); age; and records of your educational courses. If you are a current student, you can log in to your online BYU-Pathway account at any time and view student data that may have been affected.

What are we doing?

Upon discovery of the incident, we immediately initiated our incident response procedures and are actively working with external cybersecurity experts, federal law enforcement authorities, our legal team, and other leading cybersecurity professionals to investigate the incident and further enhance the security of BYU-Pathway's data and IT systems, including vendor access. This incident has been reviewed with staff, and security measures have been reemphasized to protect against similar breaches in the future. We also have notified state attorneys general, credit reporting agencies, or other regulatory authorities where legally required. If you are receiving this notice, as a precaution we are offering complimentary credit monitoring to further protect your identity. To request this service, please contact the toll-free number listed below and provide code **BYUPW25**. You will then be provided with instructions to set up credit monitoring.

What can you do?

We have no indication at this time that your personal data has been misused or published. We recommend that you remain vigilant about the security of your personal data by monitoring your personal accounts, frequently changing passwords, selecting strong and different passwords for every account, and acting on any suspicious activity. You should promptly report to your local law enforcement authorities any fraudulent activity, scam, or identity theft. In addition, you can request a credit freeze or fraud alerts associated with your personal information for free by contacting one of the major credit bureaus. By law, they are required to share that request with the other major credit bureaus.

For more information:

If you have further questions or concerns, please:

- Visit the [BYU-Pathway website](#).

- Call toll-free at **833-594-5317** (Monday–Friday, 7:00 a.m.–7:00 p.m. [MDT/UTC-6], excluding major U.S. holidays).
- Contact one of the major credit reporting agencies:
 - **Equifax**
P.O. Box 105788, Atlanta, GA 30348
1-888-298-0045 | www.equifax.com/personal
 - **Experian**
P.O. Box 9554, Allen, TX 75013
1-888-397-3742 | www.experian.com
 - **TransUnion**
P.O. Box 2000, Chester, PA 19016
1-800-680-7289 | www.transunion.com
- If you believe you are the victim of identity theft or suspect misuse of your information, you may contact the Federal Trade Commission:
 - **Federal Trade Commission**
600 Pennsylvania Ave. NW, Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
www.identitytheft.gov

If you are a resident of one of the following states, you may also access the following resources:

- **California residents:** You may also report complaints to the California Department of Justice via www.oag.ca.gov/privacy or call 1-800-952-5225.
- **District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia at databreach@dc.gov.
- **Maryland residents:** You may report complaints or obtain information from the Maryland Attorney General’s Office via ldtheft@oag.state.md.us, fax 410 -576-6566, mail to 200 St. Paul Place, Baltimore, MD 21202, or call toll-free 1-888-743-0023.
- **New York residents:** You may obtain information from the New York Attorney General’s Office at www.ag.ny.gov or call 1-800-771-7755.
- **North Carolina residents:** You may contact the North Carolina Attorney General’s Consumer Protection Division at www.ncdoj.gov or call 1-877-566-7226.

- **Rhode Island residents:** You may contact the Rhode Island Attorney General's Office at www.riag.ri.gov or call 1-401-274-4400.
- **Wyoming residents:** You may contact the Wyoming Attorney General's Consumer Protection Unit at www.ag.wyo.gov or call 1-307-777-7841.

Our top priority is the privacy and security of our students, and we are taking all necessary steps to keep your information safe. We regret any inconvenience or concern this incident may have caused.

Sincerely,

BYU-Pathway Worldwide