

# **EXHIBIT 1**

By providing this notice, Bastyr 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.

### **Nature of the Data Event**

On April 30, 2025, Bastyr learned of suspicious activity on certain systems in its environment. Upon learning this, Bastyr immediately launched an investigation with the assistance of third-party specialists to determine the nature and scope of the activity. As a result of the investigation, they determined that certain files were accessed or taken without authorization between April 23, 2025 and April 30, 2025. Thereafter, Bastyr undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected, and to whom it related. Bastyr preformed a review of the affected information as well as located address information in order to provide direct notice to affected individuals. On September 2, 2025, Bastyr confirmed the potentially impacted data contained limited information related to individuals.

The information that could have been subject to unauthorized access includes name, Social Security Number, date of birth, and diagnosis information.

### **Notice to Washington Residents**

On or about September 17, 2025, Bastyr provided written notice of this incident to two thousand six hundred seventy-six (2,676) Washington residents. 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, Bastyr moved quickly to investigate and respond to the incident, assess the security of Bastyr systems, and identify potentially affected individuals. Further, Bastyr notified law enforcement regarding the event. Bastyr is also working to implement additional safeguards and training to its employees. Bastyr is providing access to credit monitoring services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

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

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

# **EXHIBIT A**

# BASTYR UNIVERSITY

Secure Processing Center  
P.O. Box 680  
Central Islip, NY 11722-0680

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

\*\*\*Postal IMB Barcode

<<Date>>

## NOTICE OF <<DATA INCIDENT / DATA BREACH>>

Dear <<Full Name>>:

Bastyr University (“Bastyr”) writes to notify you of an incident that may affect the security of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against possible identity theft or fraud should you feel it is appropriate to do so.

**What Happened?** On April 30, 2025, Bastyr learned of suspicious activity on certain systems in its environment. Upon learning this, Bastyr immediately launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. As a result of the investigation, we determined that certain files were accessed or taken without authorization between April 23, 2025 and April 30, 2025. Thereafter, Bastyr undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected, and to whom it related. On September 2, 2025, Bastyr confirmed the potentially impacted data contained limited information related to you.

**What Information Was Involved?** The information identified in the affected files included your name and the following: <<Data Elements>>.

**What We Are Doing.** Bastyr takes the confidentiality, privacy, and security of information in its care seriously. Upon learning of the incident, we immediately commenced an investigation and took steps to implement additional safeguards and review our policies and procedures relating to data privacy and security.

We are providing you with access to <<12/24>> months of credit monitoring and identity protection services through Epiq at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to 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.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your relevant account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twenty-four (24) months. We also recommend you review the *Steps You Can Take to Protect Personal Information* section of this letter. There you will find additional information regarding ways to monitor and protect your information.

**For More Information.** If you have questions, you can call our dedicated assistance line at 877-396-3273 which is available Monday through Friday, between the hours of 6:00 a.m. and 6:00 p.m. Pacific Time, excluding major U.S. holidays. You can also write to us at Bastyr, Attn: Compliance, 14500 Juanita Dr NE, Kenmore, WA 98028.

Sincerely,

Randy C. Frisch, PhD, JD  
Chief Administrative Officer  
Bastyr University

## STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

### Enroll in Monitoring Services



Activation Code: <<Full Name>>  
<<Activation Code>>  
Enrollment Deadline: <<Enrollment Deadline>>  
Coverage Length: <<12/24>> Months

### **Epiq - Privacy Solutions ID** 1B Credit Monitoring

#### **How To Enroll:**

- 1) Visit [www.privacysolutionsid.com](http://www.privacysolutionsid.com) and click "Activate Account"
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Complete the identity verification process
- 4) You will receive a separate email from [noreply@privacysolutions.com](mailto:noreply@privacysolutions.com) confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Enter your log-in credentials
- 6) You will be directed to your dashboard and activation is complete!

**Privacy Solutions ID provides** credit monitoring through Equifax, credit report and score access, \$1 million identity theft insurance with \$0 deductible, ID Restoration services, and dark web monitoring. See below for more details.

#### **Credit Monitoring with Alerts**

Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

#### **1-Bureau Credit Score and Report<sup>1</sup>**

Annual 1-Bureau VantageScore and 1-Bureau Credit Report

#### **SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)**

Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, and payment platform, with alerts.

#### **Dark Web Monitoring**

Searches for compromised information across the dark web, with alerts.

#### **Credit Report Lock/Freeze**

Assists with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

#### **Lost Wallet Assistance**

Assistance with canceling and reissuing credit and ID cards.

#### **Identity Restoration**

Dedicated ID restoration specialists who assist with ID theft recovery.

#### **Up to \$1M Identity Theft Insurance<sup>2</sup>**

Provides up to \$1,000,000 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

#### **Unauthorized Electronic Funds Transfer- UEFT<sup>2</sup>**

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity--occurrence based.

#### **Personal Info Protection**

Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers — so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., EST.

<sup>1</sup> The credit scores provided are based on the VantageScore 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. Credit monitoring from Experian and TransUnion will take several days to begin.

<sup>2</sup> Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## **Monitor Your 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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/data-breach-help">https://www.transunion.com/data-breach-help</a>
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](http://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](http://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/>. You may call Bastyr directly at (425) 602-3000.

*For New Mexico residents*, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

*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](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.