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

Sean Hoar, Partner & Chair
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
shoar@constangy.com
Telephone: 503.376.5932

December 21, 2025

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
Tel: 206-464-6684

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents the University of Phoenix, Inc. ("University of Phoenix") in conjunction with their response to a recent data security incident discussed below. Based in Phoenix Arizona, the University of Phoenix is a subsidiary of Phoenix Education Partners, Inc. The purpose of this letter is to notify you of the incident pursuant to Washington's data breach notification statute, Wash. Rev. Code §§ 19.255.005 - 040.

1. Nature of the Security Incident

On November 21, 2025, the University of Phoenix learned that an Oracle E-Business Suite ("Oracle EBS") software vulnerability may have resulted in a cybersecurity incident. Upon detecting the incident, the University of Phoenix promptly took steps to investigate and respond with the assistance of leading third-party cybersecurity firms. On November 24, 2025, the University of Phoenix determined that, like many other organizations, including other academic institutions, an unauthorized third-party exploited a previously unknown software vulnerability in Oracle EBS to exfiltrate certain data from within the University of Phoenix's Oracle EBS environment. This exfiltration occurred between August 13 and 22, 2025.

2. Number of Affected Washington Residents & Information Involved

The incident involved personal information for approximately 64,796 Washington residents. The incident may have involved names, dates of birth, Social Security numbers, and bank account and routing numbers (without means to access).

3. Notification to Affected Individuals

Beginning December 22, 2025, letters will be sent by USPS First Class Mail to Washington residents who may have been affected. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services including 12 months of credit monitoring, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

As referenced above, upon discovering this incident, the University of Phoenix took immediate steps to investigate with the assistance of cybersecurity experts. The University of Phoenix also reported the incident to the FBI and will continue to assist them in their investigation. Finally, the University of Phoenix is in the process of notifying the potentially affected individuals and providing them with steps they can take to protect their personal information and offering the remediation services referenced above. The University of Phoenix has also established a toll-free call center through IDX to answer questions about the incident and address related concerns.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at shoar@constangy.com or 503.459.7707 or Madison Balasek at mbalasek@constangy.com or 415.918.3007.

Sincerely,

Sean B. Hoar
Partner & Chair, Cybersecurity & Data Privacy Team

Encl.: Sample Notification Letter

University of Phoenix®

Return Mail Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: March 22, 2026

To Enroll, Scan the QR Code Below:

Scan Me

Or Visit:
https://response.idx.us/uphoenix/

December 22, 2025

Subject: Notice of Data <<Variable Header: Security Incident/ Breach>>

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

We are writing to inform you of a cybersecurity incident that may have affected your personal information. The University of Phoenix, Inc. ("University of Phoenix") takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened. On November 21, 2025, we learned that an Oracle E-Business Suite ("Oracle EBS") software vulnerability may have resulted in a cybersecurity incident. Upon detecting the incident we promptly took steps to investigate and respond with the assistance of leading third-party cybersecurity firms. We determined that, like many other organizations, including other colleges and universities, an unauthorized third-party exploited a previously unknown software vulnerability in Oracle EBS to exfiltrate certain data from within the University's Oracle EBS environment. This occurred between August 13 and 22, 2025.

What Information Was Involved. The information may have included your name and <<impacted data elements, e.g., Social Security number>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We also notified law enforcement and will continue to assist them in their investigation. We also implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We are also offering you complimentary identity protection services through IDX, a leader in consumer identity protection. These services include <<Membership Offering Length: 12/24>> months of credit monitoring, dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is March 22, 2026.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through IDX by calling 1-833-353-7866, going to https://response.idx.us/uphoenix/, or scanning the QR image and using the enrollment code provided above.

The University of Phoenix, Inc.
4035 South Riverpoint Parkway
Phoenix, AZ 85040-0723

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-833-353-7866 Monday through Friday from 7:00 a.m. to 7:00 p.m. Mountain Time, excluding holidays.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Chris Lynne, President
University of Phoenix

Steps You Can Take to Help Protect Your Personal 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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incident of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

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 www.annualcreditreport.com/, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
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 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file at no cost. This 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. 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.

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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://oag.maryland.gov/
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212-416-8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.