



300 The Fenway
Boston, MA 02115

[Confidential name and address]

February 13, 2025

RE: Important Security Notification. Please read this entire letter.

A notice will be sent via both email and postal mail to ensure proper delivery

Dear [Confidential]:

Simmons University recently discovered an incident that may affect the security of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so. You are also entitled to the police report which will be filed with Simmons Public Safety.

What Happened? On or about February 5, 2025, you received a phishing email titled "Health Advisory: Ebola Case - What You Need to Know for Safety". That email contained a link which you clicked on and when prompted for your login credentials you provided them and approved a fraudulent MFA request. This allowed threat actors to login to the Simmons WorkDay system as "you" where they accessed your personal information.

What Happened? On or about February 5, 2025, you received a phishing email titled "Health Advisory: Ebola Case - What You Need to Know for Safety". That email contained a link which you clicked on and when prompted for your login credentials you provided them, and approved a fraudulent MFA request. This allowed threat actors to login to the Simmons WorkDay system as "you" where they accessed personal information.

What Information Was Involved? The threat actors had access to the personal information stored in WorkDay, such as banking information, your 2024 W2, social security number, and personal information (biological sex, DOB, age, Marital Status including date of marriage, race/ethnicity, citizenship status, nationality, gender identity, and pronouns).

What We Are Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. We continue to train people monthly on how to protect themselves against cyber-attacks such as phishing, malware, and social engineering to reduce the risk of breaches.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24-months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for 24-months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by 5/12/2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorksSM website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: [Confidential]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorksSM online, please contact Experian's customer care team at **1-877-288-8057** by **5/12/2025**. Be prepared to provide engagement number [Confidential] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorksSM. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorksSM:

- **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 ExtendCARETM**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorksSM membership has expired.
- **\$1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, feel free to reach out via email.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kristen Howard".

Kristen Howard, Information Security Officer
Simmons University

* 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.