South Dakota State University

Division of Technology & Security

SAD 208, Box 2201
South Dakota State University
Brookings, SD 57007

Phone: 605.688.4988

January 6, 2025

«FIRST_NAME» «LAST_NAME»
«STREET_1» «STREET_2»
«CITY», «STATE» «ZIP»

Dear «FIRST_NAME»,

We deeply regret to inform you about a recent data security incident that may have affected some of your personal information. Your trust is of utmost importance to us, and we are committed to protecting your data. We discovered that some of your personal information may have been exposed due to a misconfiguration of an Information Technology resource. We take your privacy seriously and want to explain what happened and what we are doing to address it. We deeply regret any inconvenience this may have caused and are committed to ensuring the security of your personal information.

What Happened?

On December 11, 2024, we discovered that files containing your Personally Identifiable Information (PII) were mistakenly made accessible to unauthorized individuals due to a misconfiguration of an Information Technology resource. Upon discovery, immediate steps were taken to block access and rectify the misconfiguration. Only individuals with valid SDSU credentials could have accessed these files between the dates of January 17, 2024, and December 12, 2024. We have no evidence that the information was misused.

What Information Was Involved?

One or more of the following data elements may have been exposed:

- First name, middle name, last name
- Date of birth
- Street address, city, state, ZIP
- Phone number
- Student ID number
- Student email address
- Personal email address
- Alternate email address
- Gender
- Educational record information related to academic history and academic goals

What We Are Doing.

We are taking steps to prevent situations like this from occurring in the future:

1. **Notification:** We have notified the Department of Education, the Attorney General and Consumer Protection offices of the states of residency of affected individuals, as required by law. Additionally, SDSU has also notified the three primary credit reporting bureaus of this situation.

2. **Enhanced Security Measures**: We have implemented additional security protocols to safeguard sensitive information stored in university information technology resources, and we are exploring additional options for protecting this data.

3. **Training and Awareness**: We are conducting comprehensive training sessions for faculty and staff to ensure they understand the importance of data security and how to protect personal information.

4. **Regular Audits**: We will perform regular audits of our data storage systems to identify and address potential vulnerabilities.

What You Can Do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

To protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days.

To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed in the "Additional Resources" section included with this letter or via their website. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each. You can also contact the Federal Trade Commission for additional information about fraud alerts or security freezes. If you suspect that you have been the victim of identity theft, report the situation to local law enforcement or your state's attorney general office.

We sincerely apologize for any inconvenience this may have caused and want to assure you that protecting your information remains SDSU's top priority.

Sincerely,

Paul Kern
Chief Information Security Officer
South Dakota State University

sdsu.security@sdstate.edu

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.