DATA INCIDENT NOTIFICATION

What Happened

Stanly Community College ("SCC") was the subject of a criminal cyberattack (the "Incident") that impacted a small number of employee email accounts. We immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope, the impact on our information systems, and the identities of those the Incident may have affected.

Through our extensive investigation, we identified a limited set of email accounts that may have been subject to unauthorized access. We then undertook the time- and resource-intensive steps of data mining and manually reviewing the contents of those accounts to determine whether they contained personally identifiable information ("PII") and to identify the data subjects to whom that PII related.

On or about July 13, 2022, we determined that, during the following periods, the threat actor(s) **may** have accessed PII in the affected email accounts that related to you: July 29, August 15-17, or August 3 to September 9, 2021. We have not found any evidence that your information was misused as a result of the Incident.

What Information Was Involved

A small number of the emails subject to the Incident contained one or multiple data elements of PII, which could include names, social security numbers, student ID numbers, online account credentials, and/or driver's license numbers.

What We Are Doing

Out of an abundance of caution, we are providing this notice so that all potentially affected individuals can take steps to minimize the risk that their information will be misused. As an added precaution, we have arranged for the provision of 12 months of free credit monitoring and related services to potentially affected individuals. To find out whether you were among those whose information was potentially affected, please contact us at 1-888-220-4909.

SCC treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, we have taken a number of steps to further secure our systems. Specifically, we have: reset all email passwords, enabled multifactor authentication for all users, upgraded the security of our email platform, implemented continuous logging, and are in the process of reviewing and updating our existing data security policies and procedures.

What You Can Do

In addition to enrolling in the free credit monitoring and related services mentioned above, we recommend that you immediately reset your username and password to all financial accounts, and that you remain vigilant and take the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
Consumer Fraud Division	Consumer Fraud Assistance	Consumer Relations & Fraud
P.O. Box 740256	P.O. Box 9556	Victim Assistance

Atlanta, GA 30374 800-525-6285 security.dataadministration@equifax.com	Allen, TX 75013 888-397-3742 businessrecordsvictimassistance@experian.com	1561 E. Orangethorpe Ave. Fullerton, CA 92831 800-372-8391 FVAD@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also report this to the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

For More Information

If you have questions or concerns, please contact us at 1-888-220-4909. We apologize for this situation and any inconvenience it may cause you.

Sincerely,

Dr. John Enamait
President
Stanly Community College

4821-1179-2860, v. 1