JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
29th Floor
New York, NY 10017
(212) 545-4063
www.jacksonlewis.com

Damon W. Silver
Direct: (212) 545-4063
damon.silver@jacksonlewis.com

VIA FIRST-CLASS MAIL
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification[1]

May 24, 2023

Dear Sir or Madam:

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

Through its extensive investigation, the College identified a limited set of employee email accounts that were subject to unauthorized access. It 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, the College determined that the threat actor(s) may have accessed PII in the affected email accounts relating to a New Hampshire resident during one of the following periods: July 29, August 15-17, or August 3 to September 9, 2021. The impacted email accounts contained

. The College found no evidence that this information was misused.

The investigation identified one (1) New Hampshire resident who may have been affected by the Incident. Out of an abundance of caution, and in accordance with applicable law, the College will provide notice to the affected New Hampshire resident, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused.

SCC worked diligently to complete its investigation and provide notice to potentially affected individuals as expeditiously as possible. Due to significant understaffing and missed work time related to COVID-19, protracted injury to a key decisionmaker, high-level personnel turnover, and

[1] Please note that Stanly Community College is not, by providing this letter, agreeing to the jurisdiction of State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

challenges related to the impacted datasets, however, SCC was not able to complete these tasks as quickly as it endeavored to.

As set forth in the enclosed letter, the College has taken numerous steps to protect the security of the personal information under its control and to prevent the occurrence of similar future incidents. Since learning of the attack, the College has: reset all email passwords, enabled multifactor authentication for all users, upgraded the security of its email platform, implemented continuous logging, and is in the process of reviewing and updating its existing data security policies and procedures.

The College will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me.

Sincerely,

JACKSON LEWIS, P.C.
/s/ Damon W. Silver

cc: Gregory C. Brown (Jackson Lewis P.C.)
Jackson E. Biesecker (Jackson Lewis P.C.)

Stanly Community College
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-888-220-4909
Or Visit:
https://response.idx.us/SCC
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

May 24, 2023

<<Incident Notice/Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>,

What Happened

We are writing to notify you that 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

The impacted email accounts contained your

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are offering identify theft protection services through IDX, A ZeroFox Company, a data breach and recovery services expert. IDX identity protection services include <<12 / 24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-888-220-4909 or going to https://response.idx.us/SCC and using the enrollment code provided above. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time. Please note that the deadline to enroll is August 24, 2023.

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 credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

If you have questions or concerns, please contact .

We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

Dr. John Enamait
President
Stanly Community College

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking 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	Experian Security Assistance	Consumer Relations & Fraud
P.O. Box 740256	P.O. Box 72	Victim Assistance
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 2000
800-525-6285	888-397-3742	Chester, PA 19016
securitymonitoring@equifax.com	businessrecordsvictimassistance@experian.com	800-372-8391
		databreach@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 contact 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

4. *For District of Columbia Residents:* You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

5. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

6. *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or

Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf

7. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

8. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.