Davis Wright Tremaine LLP

Suite 800
1919 Pennsylvania Avenue N.W.
Washington, D.C. 20006-3401

Christin McMeley
202-973-4264 tel
christinmcmeley@dwt.com

May 7, 2018

New Hampshire Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Re: Report of Data Breach

To the New Hampshire Department of Justice:

I represent DigiPen Institute of Technology ("DigiPen"), located at 9931 Willows Road NE, Redmond, WA 98052. Pursuant to N.H. Rev. Stat. § 359-C:20(I)(b), I am writing to notify you of an unauthorized disclosure of personal information involving one (1) resident of New Hampshire. We expect notice of this incident to be mailed to the affected individual on or about May 7, 2018.

On April 25, 2018, an authorized DigiPen employee inadvertently emailed a spreadsheet containing certain students' personal information to a recipient that was not authorized to access that information (as opposed to the email's intended recipient). The spreadsheet included each student's full name, Social Security numbers, student ID, and the program in which the student was enrolled. DigiPen discovered the error on April 30, 2018 and immediately initiated an investigation to determine what happened and who may have been affected. Additionally, DigiPen promptly contacted the email recipient to request that the information be returned and/or destroyed (to date, no response has been received).

Although there is no indication that the New Hampshire resident's information has been misused, DigiPen has arranged to provide one year of credit monitoring and identity theft protection services from AllClear ID at no cost to the potentially affected individuals. DigiPen continues to seek contact with the unintended recipient to request that the information be permanently deleted and to confirm that the information has not been, and will not be, shared with any third parties. DigiPen is also in the process of implementing additional measures with respect to security, including reviewing and updating their internal protocols regarding the storage and transfer of personal information, as well as additional user education designed to prevent the recurrence of a similar incident.

Please contact me should you have any questions.

Sincerely,

Christin McMeley, CIPP/US

Enclosure: Representative sample notification letter to the New Hampshire resident.

DigiPen
INSTITUTE OF TECHNOLOGY

9931 Willows Road
Redmond, WA 98052
Phone (425) 558-0299
Toll-Free (866) 478-5236
FAX (425) 558-0378

www.digipen.edu

[redacted]

May 7, 2018

Re: Notice of Data Breach

Dear [redacted]:

We are writing to inform you of an incident that may have resulted in the unauthorized acquisition of your personal information and, in an abundance of caution, are providing you with identity protection services, as described below.

What Happened?

On April 25, 2018, an authorized DigiPen employee inadvertently emailed a spreadsheet containing certain students' personal information to a recipient that was not authorized to access that information (as opposed to the email's intended recipient). We discovered the error on April 30, 2018 and immediately initiated an investigation to determine what happened and what may have been affected. We currently have no evidence to suggest that your information has been acquired or used for an unauthorized purpose, but we wanted to inform you of this incident as soon as possible out of an abundance of caution.

What Information Was Involved?

It is possible that the following personal information may have been acquired without authorization as a result of this incident: full name, Social Security number, student ID, and the program in which you enrolled.

What We Are Doing.

We are seeking contact with the unintended email recipient to request that the information be permanently deleted and to confirm that the information has not been, and will not be, shared with any third parties. Additionally, we are in the process of implementing additional measures with respect to security, including by reviewing our internal protocols regarding the storage and sharing of personal information, and will provide additional user education designed to prevent the recurrence of a similar inadvertent disclosure.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: [redacted]

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may be required in order to activate your monitoring options.

What You Can Do.

In addition to enrolling in the services described above, further information about how to guard against identity theft appears on the next page.

For More Information.

For further information, or should you have any questions, please contact Marshall Traverse, Dean of Students at 425-629-5034.

We deeply regret any inconvenience this may cause you.

Sincerely,

Jason Chu
Chief Operating Officer - International

Steps You Can Take To Further Protect Your 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 incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Obtain a Copy of Your 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 http://www.annualcreditreport.com/, calling toll-free 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Place a Fraud Alert on Your Credit Report. 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 90 days. 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 http://www.annualcreditreport.com.

Place a Security Freeze on Your Credit File. In some US states, you have the right to put a security freeze on your credit file. 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 consumer reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. 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 on Identity Theft: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of North Carolina can obtain more information from their Attorney General using the contact information below.

Federal Trade Commission	**North Carolina Attorney General**
600 Pennsylvania Ave, NW	9001 Mail Service Center
Washington, DC 20580	Raleigh, NC 27699
consumer.ftc.gov, and	ncdoj.gov
www.ftc.gov/idtheft	1-877-566-7226
1-877-438-4338	