



Lindsey Smith
100 Light Street, Suite 1300
Baltimore, Maryland 21202
Lindsey.Smith@lewisbrisbois.com
Direct: 410.525.6402

July 25, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
ATTN: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Frosh:

I represent DigiPen Institute of Technology ("DigiPen"), located in Redmond, WA, in connection with a recent data security incident described in greater detail below. DigiPen takes the protection of sensitive information very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the Security Incident.

On May 1, 2022, DigiPen experienced a data security incident that impacted access to its systems and data. Upon discovering the unauthorized activity, DigiPen immediately secured its digital environment and engaged leading cybersecurity experts to address the incident, restore operations, and conduct an investigation. DigiPen also notified the FBI and Department of Education about the incident. On June 15, 2022, the investigation determined that an unauthorized party accessed certain files and data stored on DigiPen's server. DigiPen reviewed the data and, on July 12, 2022, determined that the data contained the personal information of Maryland residents. The information accessed without authorization included names, addresses, driver's license numbers, and/or Social Security numbers.

2. Number of Maryland Residents Affected.

DigiPen will notify twenty-three (23) residents of Maryland via first class U.S. mail on July 26, 2022. A sample copy of the notification letter to be sent to the affected individuals is included with this correspondence.

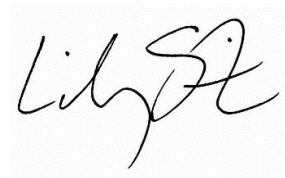
3. Steps Taken Relating to the Incident.

DigiPen has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps include working with leading cybersecurity experts to enhance the security of its systems and data.

4. Contact Information.

DigiPen remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 410.525.6402 or via email at Lindsey.Smith@lewisbrisbois.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Lindsey Smith", is centered on the page.

Lindsey Smith of

LEWIS BRISBOIS BISGAARD & SMITH
LLP

Encl: Sample Consumer Notification Letter



DIGIPEN
INSTITUTE OF TECHNOLOGY

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

To Enroll, Please Visit:

www.equifax.com/activate
Enrollment Code: <<Activation Code>>

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

[IF AG907-Adult CM]
Subject: Notice of Data Security Incident
[IFAG910-CA Adult CM]
Subject: Notice of Data Breach

Dear <<Name 1>>:

I am writing to inform you of a recent data security incident experienced by DigiPen Institute of Technology ("DigiPen"), that may have involved some of your information. We are notifying you of the incident, offering you complimentary credit monitoring and identity protection services, and informing you about steps you can take to help protect your personal information.

What Happened: On May 1, 2022, DigiPen experienced a data incident that impacted access to systems and data. Upon discovering this unauthorized activity, we immediately secured our digital environment and engaged leading cybersecurity experts to address the incident, restore operations, and conduct an investigation. Additionally, we notified the FBI and the Department of Education about the incident. On June 15, 2022, the investigation revealed that an unauthorized party accessed certain files and data stored on DigiPen's servers, which may have contained your personal information. There is no evidence that your personal information has been misused. Out of an abundance of caution, we are notifying you about the incident and providing you with complimentary credit monitoring and identity protection services.

What Information Was Involved: The data that could have potentially been accessed by the unauthorized party included your: <<Breached Elements>>

[IF AG907-Adult CM]

What We Are Doing: To help prevent something like this from happening again, we are implementing additional technical security measures. We have no indication that your information has been misused. We have taken important steps to minimize the chances of your data being misused as a result of this incident. Nonetheless, we are providing you with information about steps that you can take to help protect your personal information. As a further precaution, we are also offering you <<Cm length>> months of complimentary credit and identity monitoring services through Equifax. This product helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do: You can follow the recommendations included with this letter to help protect your information. In addition, you can enroll in Equifax's credit and identity monitoring services free of charge for <<Cm length>> months by following the instructions included with this letter. The deadline to enroll is <<enrollment deadline>>.

[IFAG910-CA Adult CM]

What We Are Doing: To help prevent something like this from happening again, we are implementing additional technical security measures. We have no indication that your information has been misused. We have taken important steps to minimize the chances of your data being misused as a result of this incident. Nonetheless, we are providing you with information about steps that you can take to help protect your personal information. As a further precaution, we are also offering you 12 months of complimentary credit and identity monitoring services through Equifax. This product helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do: You can follow the recommendations included with this letter to help protect your information. In addition, you can enroll in Equifax's credit and identity monitoring services free of charge for 12 months by following the instructions included with this letter. The deadline to enroll is <<enrollment deadline>>.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click "Submit" and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.
You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 855-925-2865 between 6am to 6pm PST, Monday through Friday.

The security of your information is a top priority for DigiPen. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Chris Comair
DigiPen Institute of Technology
9931 Willows Rd, Redmond, WA 98052

ADDITIONAL 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of 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:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>.

Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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.

How do I place a freeze on my credit reports? You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact each of the credit reporting agencies identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

How do I lift a freeze from my credit reports? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information for residents of the following states:

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400