BakerHostetler

Baker&Hostetler LLP

1170 Peachtree Street
Suite 2400
Atlanta, GA 30309-7676

T 404.459.0050
F 404.459.5734
www.bakerlaw.com

John P. Hutchins
direct dial: 404.946.9812
jhutchins@bakerlaw.com

May 22, 2019

VIA OVERNIGHT MAIL AND EMAIL
(SECURITYBREACH@ATG.WA.GOV)

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

We are writing on behalf of our client, The Georgia Institute of Technology ("Georgia Tech") and the University System of Georgia Board of Regents ("USG") – agencies of the State of Georgia, to notify your office of a security incident involving Washington residents.

In late March 2019, Georgia Tech identified signs that an unauthorized third-party had found a way to send queries through a Georgia Tech web server to an internal database that included information related to current and former students, faculty, staff, alumni, student applicants, and Affiliates of Georgia Tech. Georgia Tech's cyber security team immediately implemented its incident response protocol, took steps to secure the web server, and engaged leading forensics firms to assist in an investigation to determine the specific information in the database that was accessed and the identity of individuals whose information may have been involved. Georgia Tech notified the public and its university community on or around April 2 by posting a notice about the incident on its website and by sending an email to its constituents within the university community. Through its investigation, Georgia Tech determined that an unauthorized third party accessed the internal database between December 14, 2018 and March 22, 2019. The information in the database that may have been accessed includes name, address, Institute ID, date of birth and Social Security number.

Beginning on May 22, 2019, Georgia Tech will mail notification letters via United States Postal Service First-Class mail to the 6,698 Washington residents for which it has a mailing address, in accordance with RCW 19.255.010.[1] A copy of the notification letter is enclosed.

[1] This notice does not waive any objection by Georgia Tech or the USG that Washington lacks jurisdiction over them regarding any claims related to this incident.

Georgia Tech does not have a mailing address for every individual whose information may have involved in this incident. Georgia Tech, therefore, is unable to identify the total number of Washington residents whose information may have been subject to unauthorized access. Beginning on May 22, 2019, under RCW 19.255.010, Georgia Tech will provide substitute notification to potentially involved Washington residents by issuing a press release and posting a statement on its website. Copies of the press release and website statement are enclosed.

Georgia Tech has established a dedicated call center that individuals may call with related questions, and it is offering individuals whose Social Security numbers may have been involved with a complimentary one-year membership to credit monitoring and identity theft protection services.

To help prevent a similar incident from occurring in the future, Georgia Tech is taking steps to enhance existing security measures. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

John Hutchins

Enclosures

Georgia Institute of Technology®

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE
CARE OF
NAME
ADDRESS1
2Dcode SEQ ADDRESS2
CSZ
COUNTRY
BREAK

To Enroll, Please Call:
1-855-543-5399
Or Visit:
https://ide.myidcare.com/georgiatech
Enrollment Code: <<XXXXXXXX>>

May 22, 2019

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

The Georgia Institute of Technology ("Georgia Tech") is committed to protecting personal information. We are writing to provide an update on the security incident that we disclosed on April 2, 2019. This notice explains the incident, measures we have taken, and some steps you can take in response.

In late March 2019, Georgia Tech identified signs that an unauthorized person had found a way to send queries through a Georgia Tech web server to an internal database. Georgia Tech immediately implemented its incident response protocol, took steps to secure the web server, and began an investigation to determine what records in the database were accessed. The U.S. Department of Education was notified, and Georgia Tech set up a dedicated website on April 2, 2019 that shared its preliminary findings.

Leading forensic firms were engaged to assist in the investigation and help determine the specific information that was accessed. The investigation determined that access to the database may have occurred between December 14, 2018 and March 22, 2019. The information about you in the database that may have been accessed includes your name, address, Institute ID, date of birth and Social Security number.

As a precaution, we have secured the services of ID Experts® to offer you a complimentary one-year membership of ID Expert's MyIDCare. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. MyIDCare is completely free and enrolling in this program will not hurt your credit score. **For more information on MyIDCare, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter**. Identity restoration assistance is immediately available to you.

We regret that this incident occurred and apologize for any inconvenience. To help prevent a similar incident from occurring in the future, we are taking steps to enhance existing security measures.

If you have any questions, please call **1-855-543-5399**, Monday through Friday, **8am – 8pm**, Eastern Time.

Sincerely,

James Fortner
Executive Vice President of Administration and Finance
Georgia Institute of Technology

MyIDCare™

MYIDCARE ENROLLMENT INFORMATION

1. **Website and Enrollment.** Go to https://ide.myidcare.com/georgiatech and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-855-543-5399 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

ADDITIONAL STEPS YOU CAN TAKE

Regardless of whether you choose to take advantage of the complimentary credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. 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 Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-IDTHEFT (438-4338)

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202 www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland)1-410-576-6300 (for calls originating outside Maryland)

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or toll free at 1-877-566-7226

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit.

The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Georgia Tech Notifies Community of Security Incident

California residents click ***here***. [**LINK**]

The Georgia Institute of Technology ("Georgia Tech") has identified and taken steps to address a security incident involving personal information of certain current and former faculty, staff, students, alumni, student applicants and Affiliates. This Notification explains the incident, measures we have taken to address the security issues, and some additional steps that individuals whose information was involved in the incident can take in response.

In late March 2019, Georgia Tech identified signs that an unauthorized person had found a way to send queries through a Georgia Tech web server to an internal database. Georgia Tech immediately implemented its incident response protocol, took steps to secure the web server, and began an investigation to determine what records in the database were accessed. The U.S. Department of Education was notified, and Georgia Tech set up a dedicated website on April 3, 2019 to share its preliminary findings.

Leading forensic firms were engaged to assist in the investigation and help determine the specific information that was accessed. The investigation determined that access to the database may have occurred between December 14, 2018 and March 22, 2019. The information contained in the database that may have been accessed includes name, address, Institute ID, date of birth and Social Security number. Not every record in the database contained a Social Security number – the data that was present in a record varied depending on information provided by individuals as part of their relationship to Georgia Tech (i.e., student, faculty, staff, alumni, applicant, Affiliate)**.**

Georgia Tech is notifying 1.265 million people and offering credit monitoring and identity theft protection services to individuals whose Social Security number was involved in the incident. For individuals that have questions, Georgia Tech has established a dedicated call center where individuals may receive accurate and reliable information regarding the incident. We encourage members of our community to actively monitor for the possibility of fraud and identity theft by reviewing your credit report and credit card, bank, and other financial statements for any unauthorized activity.

We regret that this incident occurred and apologize for any inconvenience. To help prevent a similar incident from occurring in the future, we are taking steps to enhance existing security measures. If you have questions regarding this incident, please call 855-543-5399, Monday through Friday, 8:00AM to 8:00PM, Eastern Time. For information about preventing identity theft or to report suspicious activity, contact the Federal Trade Commission at 1-877-IDTHEFT (438-4338) or get free information at www.ftc.gov/idtheft.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. 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 Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov
- *Rhode Island Attorney General*, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400

If you are a resident of **Massachusetts** or **Rhode Island**, please note that pursuant to Massachusetts and Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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.

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.
To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit.

The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Media contact:
Lance Wallace
Georgia Institute of Technology
lance.wallace@comm.gatech.edu>
(404) 894-7460

Georgia Tech Notifies Community of Security Incident

ATLANTA, GA (5/22/2019) – The Georgia Institute of Technology (Georgia Tech) has identified and addressed a security incident involving personal information related to current and former faculty, staff, students, alumni, student applicants and affiliates.

Georgia Tech is notifying 1.265 million people and offering credit monitoring and identity theft protection services to individuals whose Social Security number was involved in the incident.

In late March 2019, Georgia Tech identified signs that an unauthorized person had found a way to send queries through a Georgia Tech web server to an internal database. Georgia Tech immediately implemented its incident response protocol, took steps to secure the web server and began an investigation to determine what records in the database were accessed. The U.S. Department of Education was notified, and Georgia Tech set up a dedicated website on April 2, 2019, to share its preliminary findings.

Leading forensic firms were engaged to assist in the investigation and help determine the specific information that was accessed. The investigation determined that access to the database may have occurred between December 14, 2018, and March 22, 2019. The information contained in the database that may have been accessed includes name, address, Institute ID, date of birth and Social Security number. Not every record in the database contained a Social Security number – the data that was present in a record varied depending on information provided by individuals as part of their relationship to Georgia Tech (i.e., student, faculty, staff, alumni, applicant, affiliate). For individuals who have questions, Georgia Tech has established a dedicated call center where individuals may receive accurate and reliable information regarding the incident.

“We regret that this incident occurred and apologize for any inconvenience,” said Jim Fortner, interim executive vice president for administration and finance. “To help prevent a similar incident from occurring in the future, Georgia Tech is taking steps to enhance existing security measures.”

Anyone with questions regarding this incident, should visit http://notice.gatech.edu or call 855-543-5399, Monday through Friday, 8 a.m. to 8 p.m., Eastern Time.