



Office of the Vice President and General Counsel

PO Box 100248
Gainesville, FL 32610-0248
352-273-6836
352-273-7999 Fax

August 12, 2020

Via Email (SecurityBreach@atg.wa.gov)

Office of the Attorney General
1125 Washington St. SE
PO Box 40100
Olympia, WA 98504

Re: Incident Notification

Sir or Madam:

I am writing to notify your office of a security incident involving 5,075 Washington residents. The University of Florida (“UF”) has learned of a security incident involving one of its software vendors, Blackbaud. UF utilizes Blackbaud’s cloud-based product to maintain current and accurate information about its alumni, as well as maintaining lists of former patients of UF’s clinics and hospitals operating under the name of UF Health.

On July 16, 2020, the UF received notification from Blackbaud that they had discovered a cyberattack on one of their systems that stores information. The cyberattack occurred at some point beginning on February 7, 2020 and could have been in there intermittently until May 20, 2020, when it was first discovered by Blackbaud. Once it discovered the attack, Blackbaud worked with law enforcement and an external investigator to research the incident. The cybercriminal demanded a ransom in exchange for an assurance that they would destroy the stolen data. Blackbaud paid the ransom and received confirmation that the data the cybercriminal removed from the Blackbaud system had been destroyed. Blackbaud has not disclosed the details about how

The Foundation for The Gator Nation

An Equal Opportunity Institution

the data were destroyed and what confirmation was received. Blackbaud has, however, shared that, based on their research and third-party (including both law enforcement and forensic security firms) investigations, they have no reason to believe that any data was or will be misused, or will be disseminated or otherwise made publicly available.

UF does not use this system to store highly sensitive personal or clinical information. Our research into this incident has revealed that some personal information, including demographic information (such as names, addresses, phone numbers, and e-mail addresses) was included. Additionally, dates of birth, physician names (if applicable), and visit location information (if applicable) may have also been included.

On August 12, 2020, UF began mailing notices via postal mail to Washington residents in accordance with HIPAA and RCWA § 19.255.010.¹ There were different notices from UF and UF Health, depending on which database the individual's data was stored. A copy of each of the notification letters is enclosed.

While this incident did not involve UF controlled systems, it is taking steps to evaluate its vendor's security measures, to ensure appropriate protections are in place to prevent these types of incidents from occurring with UF data.

Please don't hesitate to contact me if you have any questions.

Regards,

Andrew Eisman

Andrew B. Eisman
Senior Counsel

¹ This report is not, and does not constitute, a waiver of UF's objection that Washington lacks personal jurisdiction over it regarding any claims related to this data security incident.



University of Florida Foundation
1938 W. University Avenue
Gainesville, FL 32603

August 13, 2020

Name
Address
Address
City, WA 991XX
5019
13

Dear NAME,

As an organization dedicated to connecting individual passions with institutional priorities that improve lives and communities across our state, nation, and world, we take great pride in the trust that you place in us on a daily basis. In turn, we commit to managing your gifts of time and resources with the utmost integrity, and to communicating with you regularly about how these resources are managed.

We are writing today out of an abundance of caution to inform you of a data security incident involving a third-party vendor that may have involved your personal information. While we believe the risk to members of our community is low, we believe that the transparent sharing of information is critical to maintaining the trust you have placed in us. **It is important to note that the UF Foundation does not store credit card details, banking information, Social Security numbers, or other highly sensitive data in our database of record – those data are not involved in the incident detailed below.**

Below we are including full details of this incident as provided by Blackbaud, one of the UF Foundation's third-party service providers that was recently the victim of a ransomware attack involving many colleges and universities worldwide. Affected organizations include a number of colleges and universities in the state of Florida, as well as our peer public and leading private universities around the nation and world.

What happened?

On July 16, 2020, UF was notified of a security incident involving UF Foundation data by Blackbaud, a third-party vendor that helps the UF Foundation maintain current and accurate information about UF alumni. Blackbaud has informed us that this attack on their systems occurred at some point beginning on February 7, 2020 and lasted until May 20, 2020.

What information was involved?

As mentioned above, this incident does not involve highly sensitive personal information such as credit card details, banking information, or Social Security numbers. However, our research into this incident has revealed that personal information including names, dates of birth, degree information, spousal information, and various other biographical data was involved. Blackbaud has shared that, based on their research and third-party (including law enforcement) investigations, they have no reason to believe that any data was or will be misused, or will be disseminated or otherwise made publicly available.

What can you do?

It is best practice to regularly monitor and review your personal accounts and information to protect against any unwanted activity and the potential for identity theft. While we would like to reiterate that we believe the risks associated with this incident are low, we are also here to help. If you would like more information about this incident, please do not hesitate to contact us at data@uff.ufl.edu.

It is also considered best practice to monitor your personal credit accounts with national credit reporting agencies, and report any suspicious activities or concerns to them as soon as they are noticed. For your convenience, we are including the contact information for these credit agencies below:

<u>Name</u>	<u>Website</u>	<u>Phone Number</u>
Equifax	https://www.equifax.com/personal/credit-report-services	800-685-1111
Experian	https://www.experian.com/help/	888-397-3742
Transunion	https://www.transunion.com/credit-help	888-909-8872

We sincerely apologize for this incident and regret any inconvenience that this may cause you. Thank you for your understanding and your steadfast support of the University of Florida.

Best,

Tom Mitchell
Executive Vice President
University of Florida Foundation



C/O ID Experts
PO Box 4600
Everett WA 98204

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

COUNTRY



SEQ
CODE 2D
1GEN

BREAK

To Enroll, Please Call:

1-833-901-0914

Or Visit:

<https://ide.myidcare.com/ufhealth>

Enrollment Code: <<XXXXXXXXXX>>

August 14, 2020

Notice of Data Breach

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

University of Florida Health (UF Health) values its customers and respects the privacy and security of your information. As a precautionary measure, we are notifying our customers about a data security incident involving Blackbaud, a company which contracts with UF Health. Blackbaud was recently the victim of a ransomware attack, which may have affected certain UF Health data hosted by Blackbaud. While we believe the risk to our customers is low, we are committed to transparency and being in full compliance with the rules and laws that govern the confidentiality of your information.

It is important to note that Blackbaud reported it has no reason to believe that any data was or will be misused, or will be disseminated or otherwise made publicly available. Further, the data security incident does not involve credit card details, banking information, Social Security numbers, medical record numbers, clinical or diagnosis information, or other highly sensitive information. UF Health did not share that information with Blackbaud and, therefore, it was not involved in the data security incident.

What Happened

On July 16, 2020, UF Health was notified of a security incident involving data hosted by Blackbaud, a company that provides software tools and management resources to UF Health, as well as many other health care organizations, colleges and universities, and nonprofit corporations in the state of Florida, around the nation, and the world. In May 2020, Blackbaud discovered that cybercriminals had potentially been in their systems since February 2020 and were able to access a subset of data from a number of their clients, including UF Health.

What Information Was Involved

This incident does not involve highly sensitive personal, financial, or clinical information; however, our research into this incident has revealed that **some demographic information (such as names, addresses, phone numbers, and e-mail addresses) was included. Additionally, dates of birth, physician names, and visit location information may have also been included.**

Blackbaud reported that they met the ransom demands made by the cybercriminal and were provided with assurances that the data was destroyed. As emphasized above, Blackbaud has shared that, based on their research and investigations by law enforcement and forensic security firms, it has no reason to believe that any data was or will be misused, or will be disseminated or otherwise made publicly available.

What We Are Doing

Upon learning of this incident from Blackbaud on July 16, UF Health immediately began an investigation to understand whether any data was compromised and assess the impact, if any, to our customers, determine additional security measures being taken by Blackbaud, coordinate with our peers and Blackbaud, and understand why there was a delay between finding the breach and notifying UF Health and their other customers. We have established required and necessary communications to our customers and regulatory officials.

In addition, UF Health has hired ID Experts®, the data breach and recovery services expert, to provide you MyIDCare™ identity theft protection services. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

It is a best practice to regularly monitor and review your personal accounts and credit information to protect against any unwanted activity and the potential for identity theft. While we would like to reiterate that we believe the risks associated with this incident are low, we are also here to help. To that end, we have set up an informational website for access to current information and a call center to provide additional information and address any questions or concerns you may have.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-901-0914 or going to <https://ide.myidcare.com/ufhealth> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is November 13, 2020.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-901-0914 or go to <https://ide.myidcare.com/ufhealth> for assistance or for any additional questions you may have. We regret that this has taken place and apologize for any concern this may have caused you.

We take your privacy seriously and will continue to work diligently to protect your personal information.

Sincerely,

Heather Noughton Bokor

Heather Noughton Bokor
Compliance and Privacy
University of Florida Health

(Enclosure)



Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://ide.myidcare.com/ufhealth> 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 1-833-901-0914 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.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.