
To whom it may concern,

On August 19, 2023, an employee of The Cuba Center at The University of Alabama's email account was compromised via a phishing attack that also captured the user's MFA code. A bad actor had access to the mailbox for approximately 2 hours. While we have no indication that any users' passport information was viewed or used in any way, the opportunity for it to be seen existed, so we are notifying out of an abundance of caution.

The user responsible has received additional training.

Total persons affected: 79

MD State residents affected: 1

Data potentially exposed: Passport Number

Individuals were notified 9/29/23. A copy of the notification letter is included. We are offering 24 months of credit monitoring services. Please let me know if there are questions or concerns.

Sincerely,

Taylor B. Anderson

CISO

Office of Information Technology

[The University of Alabama](#)

A314 Gordon Palmer Hall

Box 870346

Tuscaloosa, AL 35487

Phone 205-348-6946

tbanderson@ua.edu | <https://oit.ua.edu>



Office of
Information Technology

The University of Alabama
Office of Information Technology
Box 870346
Tuscaloosa, AL 35487

<<To The Parent or Guardian of>>
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

September 29, 2023

Notice of Data Breach

Dear <<Parent or Guardian of>> <<First Name>> <<Last Name>>,

We are contacting you because of a security incident which may have resulted in unauthorized access to a document that contained personally identifiable information about you. We want to let you know what happened, what information was potentially accessible, and what we are doing to mitigate risks.

WHAT HAPPENED?

On August 19, 2023, an employee of The Cuba Center at The University of Alabama's email account was compromised. UA officials immediately conducted a scan of the employee's email account to determine if sensitive or confidential information was contained anywhere within the emails in the account. UA discovered the employee's email account contained multiple documents that included personally identifiable information of other individuals. While we have no indication that the information was viewed or used in any way, the opportunity for it to be seen exists.

WHAT INFORMATION WAS INVOLVED?

The documents in the email account contained personally identifiable information including the following:

<<variable data – Impacted data>>

WHAT YOU CAN DO.

The University is offering you two years of free credit monitoring and identity theft detection services. These services, detailed in the enclosed document, are available at no charge to you. Even if you choose not to take advantage of this free membership, we have included other additional credit safety tips you may wish to use.

WHAT WE ARE DOING.

We apologize for any inconvenience or concern this incident may cause you. We are bringing this to your attention so that you can be alert to signs of any possible misuse of your information.

Please know that the entire UA administration takes this incident seriously, and we are committed to doing all we can to keep this from happening again. The University constantly reviews and updates the comprehensive plan we have in place to secure sensitive information, and we are committed to continuing to do so, including requiring every employee to use two-factor authentication for all University email accounts.

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 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have. Representatives are available Monday through Friday, from 9 am to 9 pm Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Taylor Anderson", with a stylized flourish at the end.

Taylor Anderson
Chief Information Security Officer, The University of Alabama

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is December 29, 2023.

2. Activate the credit monitoring provided as part of your IDX identity protection 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, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 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 IDX identity protection, notify them immediately by calling or by logging into the IDX 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.