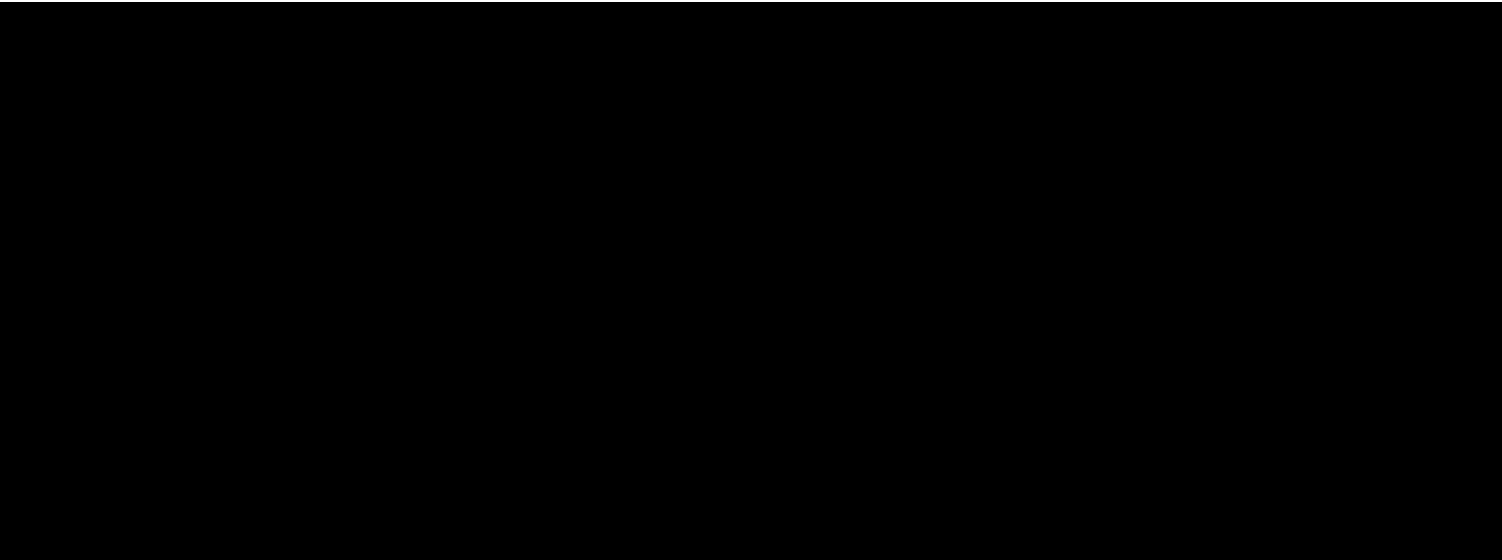




Breach Report

- Description of the information compromised:
 - A spreadsheet was uploaded on Feb 2, 2023 as a Point of Contact list, for the Technology Department of the School of Science, Technology, and Education. The spreadsheet included personally identifiable information of 364 current and former faculty and staff, including disclosure of AACC IDs for 309 individuals. The spreadsheet contained the following information:
 - Name (first, last, middle initial)
 - AACC ID number
 - Home Address (house number, street, city, state, zip)
 - Phone (home, work, cell)
 - Email address (personal, AACC)
 - Department
 - First Semester hired
 - Active/Inactive
 - FT or PT
 - Status
 - Note
 - This incident did not involve social security numbers or dates of birth
- Contact information for the business, including a toll-free number if the business has one:

Anne Arundel Community College
101 College Parkway
Arnold, MD 21012

John Williams
Director information Security
Phone: (410) 777-1255
Email: Jwilliams6@aacc.edu

- Toll-free numbers and addresses for each of the three credit reporting agencies: Equifax, Experian, and TransUnion
 - Experian**
 Online: [Experian Freeze Center](#)
 Phone: 1-888-397-3742
 By mail, write to:
 Experian Security Freeze
 PO Box 9554
 Allen, TX 75013
 - Equifax**
 Online: [Equifax Credit Report Services](#)
 Phone: 1-800-685-1111
 By mail, write to:
 Equifax Information Services LLC
 PO Box 105788
 Atlanta, GA 30348-5788
 - TransUnion**
 Online: [TransUnion Credit Freezes](#)
 Phone: 1-888-909-8872
 By mail, write to:
 TransUnion LLC
 PO Box 2000
 Chester, PA 19016
- Toll-free numbers, addresses, and websites for the Federal Trade Commission (FTC) and the Maryland Office of the Attorney General (OAG)
 - Federal Trade Commission
 - identity theft website (www.identitytheft.gov/).
 - (877)- 4338-4338
 - (866) 653-4261 (TTY)
 - Contact the OAG Identity Theft Unit
 - Phone: (410) 576-6491
 - Fax: (410) 576-6566
 - E-mail: idtheft@oag.state.md.us
 - Mail: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202
- A statement that the individual can obtain information from these sources about steps to avoid identity theft:
 - See information below
- Attach a sample copy of the notice being sent to consumers:
 - See information below

March 9, 2023

Dear [NAME]:

Notice of Data Breach

We regret to inform you that a spreadsheet, containing your name and AACC identification number, which is considered personally identifiable information, along with other information was uploaded to a Microsoft TEAMS collaboration channel. As required by Maryland law, this notice is being provided to make you aware of the potential effects of this incident. We take the security of all our employee's information very seriously and deeply regret any concern this may cause you.

What Happened

A spreadsheet was uploaded on Feb 2, 2023 as a Point of Contact list, for the Technology Department of the School of Science, Technology, and Education. The spreadsheet was accessible by thirty (30) faculty members; however, our records reflect that only four (4) faculty members accessed the information prior to the spreadsheet being removed from TEAMS on February 16, 2023. Two (2) of the faculty members who viewed the spreadsheet did not have access to the AACC ID and are considered "unauthorized" for viewing the sensitive information contained in the spreadsheet. Individuals that viewed the spreadsheet have deleted it from their computers.

What Information Was Involved

The spreadsheet contained the following information:

- Name (first, last, middle initial)
- AACC ID Number
- Address (house number, street, city, state, zip)
- Phone (home, work, cell)
- Email address (personal, AACC)
- Department
- First Semester hired
- Active/Inactive
- FT or PT
- Status
- Note

Because your AACC ID number is considered an individual identification number created by AACC, personal information was disclosed to unauthorized individuals.

What We Are Doing

As stated above, the spreadsheet has been removed from the TEAMS channel, the individuals who accessed the spreadsheet have deleted the spreadsheet from their computers and no longer have access to the information, and we are providing you, and others impacted, with notice of the incident.

What You Can Do

We recommend the following:

- Reduce your electronic internet footprint as much as possible. This includes any websites, unused email accounts and use of AACC email addresses for other websites.
- Monitor your credit reports. Your SSN and date of birth were not part of the information included in the spreadsheet, but it is always wise to review your credit report at least annually. If you are not trying to obtain credit, it is recommended to freeze your credit reports.
- Monitor emails. Extra diligence should be used to review all emails to identify spam, phishing, or fraud emails sent to your AACC or personal email addresses.
- Monitor postal mail. Extra diligence should be used to review postal mail to identify phishing or fraud mail sent to your home address.

If you are concerned that possible identity theft, or increased spam emails, or increased postal mail have occurred since Feb. 2, 2023, please contact me.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact me at 410-777-1255. I work part time remotely, so please, leave a message and I will return your phone call.

Again, we sincerely regret any concern this incident may cause.

Sincerely,

John Williams

Anne Arundel Community College

Director Information Services

Information about Identity Theft Protection

You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, <https://ncdoj.gov/protecting-consumers/identity-theft/>.

For residents of Pennsylvania: You may also obtain information from the Pennsylvania Office of Attorney general, Strawberry Square, Harrisburg, PA 17120, (717) 787-3391 or on their website: <https://www.attorneygeneral.gov/protect-yourself/identity-theft/>

For residents of South Carolina: The South Carolina Department of Consumer Affairs' Identity Theft Unit ("the Unit") aims to inform consumers about the steps they can take to protect themselves from identity theft, how to spot if they are a victim and provide tailored remediation and guidance to identity theft victims: The Department of Consumer Affairs, 293 Greystone Blvd, Suite 400, Columbia, SC 29210 (800) 922-1594 or visit the website at www.consumer.gov and click on "Identity Theft Resources."

For residents of Virginia: You may also obtain information from the Virginia Office of the Attorney General on their website: https://www.oag.state.va.us/consumer-protection/index.php?option=com_content&view=article&id=156

Security Freezes and Fraud Alerts:

You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any

subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity; and
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting->

[act.pdf,https://www.consumerfinance.gov/learnmore/](#), or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com) General Contact: P.O. Box 740241 Atlanta, GA 30374 800-685-1111 Fraud Alerts: P.O. Box 740256, Atlanta, GA 30374 Credit Freezes: P.O. Box 105788, Atlanta, GA 30348	Experian (www.experian.com) General Contact: P.O. Box 2002 Allen, TX 75013 888-397-3742 Fraud Alerts and Security Freezes: P.O. Box 9554, Allen, TX 75013	TransUnion (www.transunion.com) General Contact, Fraud Alerts and Security Freezes: P.O. Box 2000 Chester, PA 19022 888-909-8872
---	--	--

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its content, is strictly prohibited. If you have received this communication in error, please contact the sender by reply email and destroy all copies of the original message. Thank you.