## Breach Report

- **Description of the information compromised:**

AACC received a fraudulent application to attend the college in January 2024. During the normal admission process, the application was flagged for additional identity verification. We received a photo of a Maryland Driver's License, complete with picture, name, date of birth, and address. When the college processed the application, it linked the fraudulent application with a previous student account from 2010. The prospective student's name, address, date of birth and social security number were provided by the perpetrator during the fraudulent application and validation process. Because the information provided by the perpetrator was validated and matched against a previous account, the systems assigned an old account to the fraudulent application. The previous student's account had been deleted after 5 years of no activity, therefore, a new account was created, but the previous AACC ID number, Username and AACC email address was provided to the fraudulent applicant.

The information provided by the fraudulent applicant includes:

- Name
- Address
- Date of Birth
- Social Security Number
- Email address
- Phone number
- Emergency Contact

Information in the previous student's account available to the perpetrator, in addition to the above, includes:

- Courses taken
- Grades
- School terms attended
- Academic Program
- College Advisors and Counselors
- High School attended
- High School Graduation Date

- **Contact information for the business:**

  Anne Arundel Community College
  101 College Parkway
  Arnold, MD 21012

  John Williams
  Director Information Security
  Phone: (410) 777-1255
  Email: [Jwwilliams6@aacc.edu](mailto:Jwwilliams6@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 attachment
- **Attach a sample copy of the notice being sent to consumers:**
    - See attachment

John Williams, CISSP
Director Information Security
**Information and Instructional Technologies Division**
**Anne Arundel Community College**

July 18, 2024

[redacted]

Dear [redacted]

Anne Arundel Community College (AACC) has identified a security incident that involved access to some of your personal information. We are informing you of the incident, steps we have taken in response, and resources available to help you protect your information. We take the security of employee and student information very seriously and deeply regret any concern this may cause you. AACC is offering to reimburse you for one year of credit and personal identification monitoring services at all 3 major credit bureaus.

***What Happened***

AACC received a fraudulent admission application using your name to attend the college in January 2024. During the routine admission process, the application was flagged for additional identity verification. The perpetrator submitted a photo of a Maryland driver's license, complete with picture, name, date of birth, and address. When the college processed the January 2024 application, our system linked the new application with your student account from 2010. Your name, address, date of birth and social security number were provided by the perpetrator during the January 2024 application and validation process. Your original account had been deleted after 5 years of inactivity, therefore, a new account was created, but the previous AACC ID number, Username and email address was assigned to the new account.

*We have since been able to ascertain that information provided in the January 2024 application was used to request financial aid by the perpetrator. AACC has canceled the financial aid and tuition and fee charges associated with the fraudulent spring 2024 activity and reported the incident to the Department of Education.*

***What Information was Involved***

The perpetrator provided the college with your personal information, and we have a reasonable belief that your personal information was stolen and being used without your knowledge. Information about your attendance at AACC in your previous account was available to the individual perpetrating this fraud.

*The information about your identity provided by the perpetrator includes:*

- *Name (matched)*
- *Address (matched)*
- *Date of Birth (matched)*

- *Social Security Number (matched)*
- *Email address (new)*
- *Phone number (new)*
- *Emergency Contact (new)*

*Because the information provided by the perpetrator was validated and matched against your previous account, information about your previous attendance at AACC was available to the individual perpetrating this fraud.*

*Previous information in your account, available to the perpetrator, in addition to the perpetrator provided information above, includes:*

- *Courses taken*
- *Grades*
- *School terms attended*
- *Academic Program*
- *College Advisors and Counselors*
- *High School attended*
- *Hight School Graduation Date*

***What We Are Doing***

We take the privacy of employee and student information seriously. We have notified the Maryland Office of the Attorney General and Department of Education about this incident. We are notifying you, through this letter, that your identity was previously stolen and was used to commit fraud. AACC is offering to reimburse you for one year of credit and personal identification monitoring services at all 3 major credit bureaus. We encourage you to take full advantage of this service. AACC also recommends taking the steps below.

***What You Can Do***

- Contact the Federal Trade Commission (FTC) online at IdentityTheft.gov or call 1-877-438-4338.

- Sign up for credit and Identity Protection – If you are interested in credit monitoring, AACC will be happy to assist you with the process. For more information, please contact Candy Chaney via email at cmchaney2@aacc.edu.

  If you prefer to sign up for credit and identity protection on your own, you can choose from the following companies:
  - Identity Force: https://secure.identityforce.com/sales_landing; (800) 719-4187
  - LifeLock: https://lifelock.com; (800) 416-0599
  - ID Watchdog: https://idwatchdog.com; (800) 970-5182
  - MyIDCare: https://www.myidcare.com; (800) 939-4170

- **Notify banks and credit card companies –** Let your financial institutions know that your identity has been stolen. This can be done without a police report, but you may also request an investigation by the police department. Obtain new credit cards, destroying the old cards, with approval from the issuing institution.

- **Inform your employer**- let your employer know that your identity has been stolen and review any request for changing information about your pay and benefits. All new information should be analyzed and reversed to the information you desire.

- **Inform your family-** although it may be embarrassing and hard. Letting others know that any emails, letters, phone calls, SMS text may not have come from you and should be deleted/ignored/blocked.

- **Inform the Department of Motor Vehicles –** an altered version of your driver's license was used to provide information. Obtain a new driver's license and they will alert appropriate agencies that the card is fraudulent.

- **Review your credit and store accounts** – Online banking allows you to identify if there are any discrepancies or unusual activity in real time. Remain vigilant and continue to monitor your accounts for unusual activity going forward. If you see something you do not recognize, immediately notify the financial institution as well as the proper law enforcement authorities. In instances of credit or debit card fraud, it is important to note that cardholders are not typically responsible for any fraudulent activity that is reported in a timely fashion.

- **Review credit reports** - We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. You may also wish to place a fraud alert or credit freeze on your credit files. Please review the "Information about Identity Theft Protection" for additional information about these options.

- **Additional Resources** - Included with this letter is a reference guide: "Information about Identity Theft Protection", which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

***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 or via email at jwwilliams6@aacc.edu.

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

John Williams, CISSP
Director Information Security
Anne Arundel Community College

# 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 (4384338), 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.

**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 some, or 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.

For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reportingact.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)<br>**General Contact:**<br>P.O. Box 740241<br>Atlanta, GA 30374<br>800-685-1111<br>**Fraud Alerts**:<br>P.O. Box 740256, Atlanta, GA 30374<br>**Credit Freezes**:<br>P.O. Box 105788, Atlanta, GA 30348 | Experian (www.experian.com)<br>**General Contact:**<br>P.O. Box 2002<br>Allen, TX 75013<br>888-397-3742<br>**Fraud Alerts and Security Freezes:**<br>P.O. Box 9554, Allen, TX 75013 | TransUnion (www.transunion.com)<br>**General Contact, Fraud Alerts and Security Freezes:**<br>P.O. Box 2000<br>Chester, PA 19022<br>888-909-8872 |