[redacted]

From: Williams, John W <jwwilliams6@aacc.edu>
Sent: Wednesday, October 16, 2024 5:00 PM
To: IDTheft
Cc: President & VPs; Boykin, Tiffany, F; Little, Andrew P.; Baum, Dan, B; Rees, Michael, A; Borders, Christopher, P; Judy, Megan, E
Subject: Breach Report
Attachments: 2024 10-3 Affected Individual Notification - T. Callinan-V2 (1).docx

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Data breach

Breach Report

- Description of the information compromised:
  - In 2 separate incidents, bad actors called the service desk to modify the phone number associated with multifactor authentication on 2 different accounts. The service desk asked identity verification questions, which were answered correctly, then changed the phone numbers, as requested. The bad actor then changed the password on the accounts. The bad actor(s) then went into the self-services system and changed banking information for each of the 2 accounts.
  - These incidents were identified when the paychecks were not received correctly on pay day.
  - The compromised account process was completed, removing the bad actor(s) from further access to the accounts.
  - Paychecks were provided through alternate methods.
  - Banking information was corrected for each account
  - Investigation concluded that the identity information was stolen from 2 individuals and then used to answer knowledge-based verification questions that were posed by the technical call center to authenticate the caller. The bad actor could have accessed sensitive information in email or Self Services system for 760 individuals.

- 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: 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

AACC | Division of Information and Instructional Technology

To: [redacted]

From: Dr. Richard C. Kralevich
Vice President for Information and Instructional Technology
Anne Arundel Community College
101 College Parkway - Arnold, MD 21012

Date: October 5, 2024

Subject: Affected Individual Notification – [redacted]

This document is to provide an update on the Division of Information and Instructional Technology's (IIT) ongoing investigation into your compromised AACC employee account. While the investigation is still in progress, we are committed to maintaining full transparency regarding the situation, the steps we are taking, and our ongoing efforts to safeguard the security of our staff, systems, and data.

What happened / What was involved?

- On 09/20/2024, [redacted] reported that he did not receive a paycheck.
- Upon receiving the automated payroll direct deposit notification, [redacted] determined the account details listed did not match his account.
- He informed various departments, including IIT, Human Resources, and Disbursements, of the incident. This prompted an investigation.
- IIT's investigation determined that a bad actor called the IIT Technical Service Desk (TSD) on 09/09/2024 at 10:56 a.m.
    - The bad actor successfully answered the identity verification questions, at which time the TSD enabled a password reset and changed the MFA phone number.
    - The bad actor then used the self-service password reset capability to change the password on [redacted]s account, log in, and changed his reimbursement and payroll bank accounts.
- Colleague sent four emails to [redacted]s aacc.edu account informing him of the banking change. Please note that some of these notifications may have been deleted by the bad actor.

- Login logs show [redacted] successfully logged into the M365 system using MFA at 1:21 p.m. on 9/9/2024.
  - At that time, he successfully changed his password without IIT assistance.
  - However, he did not change the phone number for MFA.
  - Because MFA was not reset, IIT believes this created an unknow back and forth between [redacted]s resets and the bad actors counter resets.
- Upon being notified of the issue on 9/20/2024, the TSD immediately reset [redacted]s password and phone number for MFA. This locked the bad actor out.
- Bank of America returned the funds to AACC based on the College's timely fraud alert.
- On 09/24/2024, [redacted] changed his self-service direct deposit information back to his preferred values.
- On 09/25/2024, [redacted]s paycheck was reissued.

Why did this happen?

This occurred because the cybercriminal used stolen personally identifiable information (PII) from an unknown third-party source to gain unauthorized access and impersonating legitimate users.

Next Steps:

IIT remains committed to transparency and will continue to provide updates as more information becomes available. We are confident that the threat posed by the bad actor has been effectively mitigated. As an additional protective measure, IIT has engaged Zaviant, a leading information security firm, to conduct a thorough review of the situation and ensure all necessary safeguards are in place. IIT is in the process of:

- Partnering with Zaviant to conduct a secondary forensic investigation and After-Action Report.
- Conducting a review security practice and provide additional training where necessary.
- Producing automated daily report identifying all faculty and staff password change tickets received.
- Generating all the proper notifications related to this situation.
- Conducting a security reminder training campaign in which we encourage all employees to remain vigilant, and continue following best practices for information security, such as:
    - Be cautious with email attachments or links from unknown sources
    - Report any suspicious activity to IIT
    - Ensure they are following the latest security guidelines outlined by IIT
- Improving IIT security situation management processes, protocols, and leadership structure by:
  - Assessing and streamlining current procedures for detecting, reporting, and addressing security situations and ensure protocols are aligned with industry best practices and regulatory requirements.

  - Reviewing structures to confirm responsibilities are clearly defined, and key decision-makers are empowered to act quickly in response to critical situations.
  - Evaluating communication channels to ensure timely and clear information flow both within the IIT division and across the College during an information security situation.
  - Ensuring all team members are regularly trained in situation response and are aware of their roles in the event of a security issue.

What can you do? (Credit Monitoring Resources)

We understand this situation may cause concern. To assist you, the College is offering credit monitoring for you and your family for one year. We encourage you to take full advantage of this service. Options include:

- Experian: www.experian.com - Phone: 1-888-397-3742
- Equifax: www.equifax.com - Phone: 1-888-548-7878
- TransUnion: www.transunion.com - Phone: 1-833-395-6938
- IdentityForce: www.identityforce.com - Phone: 1-877-694-3367
- myFICO: www.myfico.com - Phone: 1-800-319-4433
- LifeLock by Norton: www.lifelock.com - Phone: 1-800-543-3562
- PrivacyGuard: www.privacyguard.com - Phone: 1-800-374-8273
- IDShield: www.idshield.com - Phone: 1-888-807-0407
- IdentityIQ: www.identityiq.com - Phone: 1-877-875-4347
- ID Watchdog: https://idwatchdog.com - Phone: 1-800-970-5182
- MyIDCare: https://www.myidcare.com - Phone: 1-800-939-4170

What do I do if I have questions?

For more information or support with the credit monitoring process, please don’t hesitate to contact:

- Candy Chaney via email at cmchaney2@aacc.edu or by phone at 410-777-2487.
- Rick Kralevich via email at rckralevich@aacc.edu or by phone at 410-777-2195.
- You can also contact our IIT Technical Service Desk at 410-777-HELP (4357) or by visiting MyAACC.

Your Privacy Matters

IIT remains committed to protecting your privacy and will keep you informed as we continue to take steps to safeguard your information. The safety of our systems and data is essential to our success, and we take this responsibility seriously. Thank you for your continued cooperation and understanding as we resolve this matter and sincerely regret any concern this incident may cause. If you have any questions, please do not hesitate to contact AACC directly.

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 Free credit report, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

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), How to recover from identity theft | Consumer Advice (ftc.gov)

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, Maryland Attorney General - ID Theft

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:

Identity Theft and Online Security

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